Software Freedom
Law Center

Fall Conference
at Columbia Law School

CLE materials

November 1st, 2019

Information Regarding New York CLE Credits:

Columbia Law School has been certified by the New York State Continuing Legal Education (CLE) Board as an Accredited Provider of CLE programs. Under New York State CLE regulations, this live non-transitional CLE Program will provide 6.5 credit hours that can be applied toward the Areas of Professional Practice requirement. This CLE credit is awarded only to New York attorneys for full attendance of the Program in its entirety. Attorneys attending only part of the program are not eligible for partial credit. Attendance is determined by an attorney's sign-in and sign-out, as shown in the Conference registers. On final sign-out, attorneys should also submit their completed Evaluation Form, provided at the Conference. Please note the NYS Certificates of Attendance will be sent to the email address as it appears in the register unless otherwise noted there."

Contents

Part I

Software Fast and Slow

Chapter 1

Debian Social Contract

Debian Social Contract

Version 1.1 ratified on April 26, 2004. Supersedes Version 1.0 ratified on July 5, 1997.

Debian, the producers of the Debian system, have created the **Debian Social Contract**. The Debian Free Software Guidelines (DFSG) part of the contract, initially designed as a set of commitments that we agree to abide by, has been adopted by the free software community as the basis of the Open Source Definition.

"Social Contract" with the Free Software Community

1. **Debian will remain 100% free**

   We provide the guidelines that we use to determine if a work is *"free"* in the document entitled *"The Debian Free Software Guidelines"*. We promise that the Debian system and all its components will be free according to these guidelines. We will support people who create or use both free and non-free works on Debian. We will never make the system require the use of a non-free component.

2. **We will give back to the free software community**

   When we write new components of the Debian system, we will license them in a manner consistent with the Debian Free Software Guidelines. We will make the best system we can, so that free works will be widely distributed and used. We will communicate things such as bug fixes,

improvements and user requests to the *"upstream"* authors of works included in our system.

3. **We will not hide problems**

   We will keep our entire bug report database open for public view at all times. Reports that people file online will promptly become visible to others.

4. **Our priorities are our users and free software**

   We will be guided by the needs of our users and the free software community. We will place their interests first in our priorities. We will support the needs of our users for operation in many different kinds of computing environments. We will not object to non-free works that are intended to be used on Debian systems, or attempt to charge a fee to people who create or use such works. We will allow others to create distributions containing both the Debian system and other works, without any fee from us. In furtherance of these goals, we will provide an integrated system of high-quality materials with no legal restrictions that would prevent such uses of the system.

5. **Works that do not meet our free software standards**

   We acknowledge that some of our users require the use of works that do not conform to the Debian Free Software Guidelines. We have created "`contrib`" and "`non-free`" areas in our archive for these works. The packages in these areas are not part of the Debian system, although they have been configured for use with Debian. We encourage CD manufacturers to read the licenses of the packages in these areas and determine if they can distribute the packages on their CDs. Thus, although non-free works are not a part of Debian, we support their use and provide infrastructure for non-free packages (such as our bug tracking system and mailing lists).

The Debian Free Software Guidelines (DFSG)

1. **Free Redistribution**

   The license of a Debian component may not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license may not require a royalty or other fee for such sale.

2. **Source Code**

   The program must include source code, and must allow distribution in source code as well as compiled form.

3. **Derived Works**

   The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.

4. **Integrity of The Author's Source Code**

   The license may restrict source-code from being distributed in modified form **only** if the license allows the distribution of "`patch files`" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software. (*This is a compromise. The Debian group encourages all authors not to restrict any files, source or binary, from being modified.*)

5. **No Discrimination Against Persons or Groups**

   The license must not discriminate against any person or group of persons.

6. **No Discrimination Against Fields of Endeavor**

   The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

7. **Distribution of License**

   The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

8. **License Must Not Be Specific to Debian**

   The rights attached to the program must not depend on the program's being part of a Debian system. If the program is extracted from Debian and used or distributed without Debian but otherwise within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the Debian system.

9. **License Must Not Contaminate Other Software**

   The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be free software.

10. **Example Licenses**

    The *"**GPL**"*, *"**BSD**"*, and *"**Artistic**"* licenses are examples of licenses that we consider *"free"*.

The concept of stating our "social contract with the free software community" was suggested by Ean Schuessler. This document was drafted by Bruce Perens, refined by the other Debian developers during a month-

long e-mail conference in June 1997, and then accepted as the publicly stated policy of the Debian Project.

Bruce Perens later removed the Debian-specific references from the Debian Free Software Guidelines to create "The Open Source Definition".

Other organizations may derive from and build on this document. Please give credit to the Debian project if you do.

Back to the Debian Project homepage.

This page is also available in the following languages:

عربية (Arabiya) Български (Bəlgarski) català česky dansk Deutsch
Ελληνικά (Ellinika) español فارسی (Farsi) français Galego hrvatski Italiano
עברית (ivrit) 한국어 (Korean) magyar Nederlands 日本語 (Nihongo) norsk (bokmål)
polski Português Русский (Russkij) slovenčina suomi svenska Tiếng Việt Türkçe
українська (ukrajins'ka) 中文(简) 中文(HK) 中文(繁)
How to set the default document language

Home

About
Social Contract
Code of Conduct
Free Software
Partners
Donations
Legal Info
Data Privacy
Contact Us
Help Debian
Site map
Search
The Debian Blog

Getting Debian
Network install
CD/USB ISO images
CD vendors
Pre-installed
Pure Blends
Debian Packages
Developers' Corner

News
Project News
Events
Documentation
Release Info
Installation manual
Debian Books
Debian Wiki

Support
Debian International
Security Information
Bug reports
Mailing Lists
Mailing List Archives
Ports/Architectures

Chapter 2

Debian Free Software Guidelines Frequently Asked Questions (Pearlmutter et al.)

DFSG and Software License FAQ (Draft)

1. **Q: What is the purpose of this DFSG FAQ?**

   A: To answer common questions about the Debian Free Software Guidelines and how we judge whether some piece of software is free.

2. **Q: What is *debian-legal*?**

   A: Debian-legal is a Debian mailing list for the discussion of legal questions related to Debian, including in particular whether some package or prospective package is free software. This usually depends on the license under which it is distributed.

3. **Q: Why does it matter whether something is free software?**

   A: Debian only includes free software. So aside from all its other wonderful properties, if something is not free software (by our standards) we will not include it in Debian.

4. **Q: What makes something *free software*? Does this depend solely on its license?**

   A: To us, software freedom is a set of rights (free as in speech) rather than a price (free as in beer). There have been a number of attempts to codify these freedoms, which include the freedom to modify and distribute. For our purposes, it must conform with the Debian Free Software Guidelines. The same ideals are expressed in the *Open Source Definition* and the Free Software Foundation's *Four Freedoms*.

   This almost always depends on the license under which the software is distributed, but there are rare exceptions. When necessary we take other considerations into account. So two packages with the same license could be judged differently based on extra-license comments the copyright holder has made regarding intent or interpretation, or based on how the contents of the package interact with license stipulations.

   For a concrete example, the PINE mail client version 3.91 had an MIT-style license, which is generally considered free. The copyright holder told us they wished to interpret the license text in a somewhat counterintuitive fashion: the license allows modification and distribution, but the copyright holder said they interpreted this as allowing modification, and allowing distribution of unmodified copies, but as not allowing distribution of modified copies. We respected their wishes, considered the software non-

free, and removed it from Debian.

5. **Q: Which license is best for my new previously-unreleased software? Which should I use? I think it would be fun to make up my own!**

   A: We are computer programmers, so we appreciate the fun to be had by trying to stretch the rules or game the system. And it certainly sounds fun to write your own license! But it is our strong and heartfelt advice that using a tried-and-true license is best for almost all purposes. Even large corporations with dozens of lawyers on staff itching to write their own license have found this out the hard way, as in the Mozilla license saga, or the Djvu license story, or the trouble Trolltech had with the Qt license.

   There are many advantages to using standard licenses: they're better understood by the community, were written by actual lawyers and already vetted by the community, people do not have to spend time figuring them out before using the program or helping with development, and they make it much easier to share code between your project and others.

   In our opinion (and please do not consider this formal legal advice) ...

   - If you want to make sure that everyone who gets a binary, even a modified binary, can get a copy of the corresponding source, then the GNU General Public License, or *GNU GPL*, is almost certainly your best bet. As a practical matter the GPL has proven amazingly successful, both at encouraging communal development of software and at seeing changes sent back to the originators. (Programs available under the GPL include the Linux kernel, GNU Emacs, GCC, Mozilla, KDE, GNOME, the OpenOffice suite.)
   - If you want your code to be reusable in all free software projects, no matter which license they use, and are willing to accept the possibility that somebody may “take it proprietary” (i.e. sell binaries based on modified source without distributing the modified source and without allowing the person who bought a copy of the binary to in turn give a copy to anyone else), you should consider the “new BSD license” (also called the “BSD license without the advertising clause”) or the “MIT X license”. These BSD-style licenses make it clear that you hold copyright and make no warranty, but that is about it. These licenses are compatible with most licenses, including the GPL. Programs under BSD or BSD-like licenses include the core of the FreeBSD system (both kernel and utilities), X, many networking utilities, and the Apache web server.
   - If your code is actually a library or a plugin you might want to consider the GNU LGPL, which allows your code to be linked into proprietary software but keeps your code itself free, and is GPL compatible. (Programs available under the LGPL include BOCHS, many of the GNOME libraries, ADOLC, GLIBC, and libg++.)

Other people who have investigated these issues give similar advice. For instance, see the essay *Make Your Open Source Software GPL-Compatible. Or Else.* by David A. Wheeler, which includes some compelling statistics.

6. **Q: I've flouted your advice and written a new license. I strongly believe that it conforms to the DFSG and is a free software license. People on debian-legal don't seem to agree though. They give explanations for their decision which I find completely unconvincing. I keep trying to explain the flaws in their reasoning to them, but to no avail. Is there any way for me to compel Debian to accept that my license is free?**

   A: No.

7. **Q: I'm writing documentation to accompany a free program. What license should I use for this documentation?**

   A: We strongly suggest you use the same license as used for the program. Then it will be possible to take code and put it into the documentation, and vice versa.

   If you would like to grant some extra freedoms for the documentation not granted for the remainder of the software package (eg freedom to distribute as a paper manual without corresponding document source) we recommend you use a dual license: one of which grants these extra freedoms, and the other the same license as the program.

8. **Q: Should I use the *GFDL* for documentation I write?**

   A: The GFDL (version 1.2) seems designed mainly for book-length printed documents rather than digital materials. We would strongly recommend against use of the GFDL v1.2 (GNU Free Documentation License version 1.2), for a number of reasons. A summary of issues with the GFDL was compiled by Manoj Srivastava. If you must use the GFDL for some reason (eg for compatibility), we would very much encourage you to place the material under a dual license, like GFDL/GPL.

   It is Debian's hope that a future version of the GNU FDL can be crafted which will address the issues mentioned above, making this question moot.

9. **Q: How can I tell if a license is a *free software license*, by Debian's standards?**

   A: The process involves human judgement. The DFSG is an attempt to articulate our criteria. But the DFSG is not a contract. This means that if you think you've found a loophole in the DFSG then you don't quite understand how this works. The DFSG is a potentially imperfect attempt to express what free software means to Debian. It is not something whose

letter we argue about. It is not a law. Rather, it is a set of *guidelines*.

That said, the DFSG is a good start. You might also consider a few thought experiments which we often apply. But do keep in mind that passing some set of tests is not all there is to freeness. These tests are not the final word either: some other tricky bit of nonfreeness might be invented which is not covered by any of our current tests, or something might fail a test as it is currently worded but still be determined to be free software.

a. The *Desert Island* test.

   Imagine a castaway on a desert island with a solar-powered computer. This would make it impossible to fulfill any requirement to make changes publicly available or to send patches to some particular place. This holds even if such requirements are only upon request, as the castaway might be able to receive messages but be unable to send them. To be free, software must be modifiable by this unfortunate castaway, who must also be able to legally share modifications with friends on the island.

b. The *Dissident* test.

   Consider a dissident in a totalitarian state who wishes to share a modified bit of software with fellow dissidents, but does not wish to reveal the identity of the modifier, or directly reveal the modifications themselves, or even possession of the program, to the government. Any requirement for sending source modifications to anyone other than the recipient of the modified binary---in fact any forced distribution at all, beyond giving source to those who receive a copy of the binary---would put the dissident in danger. For Debian to consider software free it must not require any such “excess” distribution.

c. The *Tentacles of Evil* test.

   Imagine that the author is hired by a large evil corporation and, now in their thrall, attempts to do the worst to the users of the program: to make their lives miserable, to make them stop using the program, to expose them to legal liability, to make the program non-free, to discover their secrets, etc. The same can happen to a corporation bought out by a larger corporation bent on destroying free software in order to maintain its monopoly and extend its evil empire. The license cannot allow even the author to take away the required freedoms!

10. **Q: Does the DFSG apply only to computer programs?**

    A: No, we apply our standards of freedom to all parts of all software in Debian. This includes computer programs, documentation, images, sounds, etc.

The text of licenses themselves in general need not be free, although legal wording itself is often not subject to copyright and hence effectively in the public domain. Although this is a subject of some controversy within the project, in practice sometimes tiny little snippets of non-free text, generally of historic or humorous or intellectual value, are included (eg /usr/share /emacs/21.3/etc/{JOKES,MOTIVATION}). These should not be integral parts of the package, nor included in a non-removable fashion, nor constitute functional parts of the package such as code or documentation. In general we would suggest avoiding such things, but you do not have to go to enormous trouble to find and root them out. In a similar vein, sometimes relevant scientific papers or technical reports of unclear copyright status are included; although they are not approved, there has, as of yet, been no systematic effort to find and remove such manuscripts.

We do not consider any of this a precedent for the inclusion of non-free code or documentation.

11. **Q: If something is free software according to Debian's standards, do I still face legal risks when I use, modify or distribute it?**

    A: You should take this answer as a total disclaimer of everything.

    Even if we were lawyers (which we are not) neither this document nor Debian's acceptance of some license or inclusion of some software should be taken as legal advice. If you need legal advice, you need to hire your own attorney.

    We sincerely hope you don't face any serious risks, but our process does not guarantee this. In truth, no process could. As stated above, Debian mainly looks at the license accompanying some software to decide whether it meets the project's standards for free software. This leaves open a number of avenues through which legal problems might conceivably arise, including:

    - Some software might have been misappropriated, and a license applied to it without approval of the actual copyright owner. In this case, Debian's evaluation was based on false premises.
    - Some software might include code which is copyrighted by third parties and not released under a free software license, or the license terms might be violated (e.g. if they are incompatible with other license requirements). Debian only examines the license and does not formally audit the code, so this cannot be reliably detected, particularly if the problematic code were copied without attribution. (In a few cases such license violations have in fact been found, in particular incompatibilities between requirements for advertising and the GPL.)
    - Some software might infringe trademarks. Distributors could potentially be held liable for this in some jurisdictions. Currently,

Debian does not check for trademarks and their misuse.
- Some software might infringe patents in jurisdictions in which so-called software patents are allowed. Even though only end users actually run the software, and distributors do not in fact actually engage in the patented process, distributors might be held liable in such a jurisdiction. Debian makes no serious attempt to check for patent violations, and handles this issue in a haphazard and case-by-case fashion. (In fact, checking for this is in practice impossible. If everyone checked for software patents, all software production would grind to a halt.)
- Use or possession of some software might be illegal in some jurisdictions.
- Distribution of some software might be controlled by import or export restrictions in some jurisdictions.
- We might have misread or misinterpreted the license.

Debian's conclusion that a particular computer program is free software, and our choice to distribute it, is an evaluation made for our own purposes. It is not a legal statement on which you can rely, either as a user, software developer, or distributor. We do our best, but we are not lawyers. *We are unpaid volunteers. We make no guarantees.*

12. **Q: People put the darndest things in their licenses. Could you explain their impact on the freedom of the license?**

    A: Sure, here are some examples:

    a. “Send me a postcard if you like this software.”

       This makes the license non-free.

    b. **Q: But I'd like users of my software to send me a postcard, so I can get a collection of postcards from cool places!**

       A: So-called *postcardware*, or similarly *emailware* which requires users to send email to the author, fails the *Desert Island* test, so it is not free. So no: you can't put this in the license. However we understand your desire to receive postcards from users, and would like suggest another way to achieve this goal. Instead of making this a *requirement* in the license, make it a personal request. Just add a personal note from the author, which is clearly not part of the license itself, saying “Although it is not required, I'd very much appreciate it if users would send me postcards telling me how they are making use of this program.” You should still get postcards, but they will be voluntary. Which is actually nicer, when you think about it.

    c. “If you distribute this software, you must pet a cat.”

This makes the license non-free, and is also cruel to people who are allergic to cats.

d. “You may modify this software, but all bug fixes must be sent to the author.”

   This makes the license non-free. (But a request rather than a demand is fine.)

e. **Q: Are *clickwrap* licenses okay? (Meaning licenses require anyone receiving the software to click on an *“I AGREE”* button indicating ascent to the terms.)**

   A: No, not unless the clickwrap stuff can be removed. Even aside from freeness, as a practical matter such a clickwrap requirement would be an unreasonable burden upon our users.

   To be technical, in principle one could put the GPL in a clickwrap and the license would be perfectly fine. But once you add a requirement that the software must be distributed via the clickwrap, or that clickwrap code cannot be removed from the software, your license becomes non-free. Since clickwraps without such a requirement are a bit pointless, clickwrap licenses are almost always non-free.

f. **Q: I've just made up a new license which requires people using the software to agree to a contract which forbids them from doing some bad stuff (like finding security flaws and not reporting them) that copyright law would otherwise allow as fair use. We can force everyone to cooperate even more! Isn't that a great idea?**

   A: We do not think so. Such a license does not meet our standards of freedom. Freedom means not only the freedom to modify, and to help others; it also means the freedom to enjoy one's own privacy.

g. **Q: I'm a working scientist, and would like to release code implementing my work. However I want to make sure that people using the software mention its use, and cite my papers, in papers they write. Should I include this in the license?**

   A: You have a valid concern. Computer scientists often receive inadequate credit for their scientific contributions. But putting such a clause in the license would render your software non-free. Instead we suggest a note, not part of the license itself, reminding users of the rules of scientific propriety. Eg:

   > SCIENTISTS: please be aware that the fact that this
   > program is released as Free Software does not excuse you

> from scientific propriety, which obligates you to give appropriate credit! If you write a scientific paper describing research that made substantive use of this program, it is your obligation as a scientist to (a) mention the fashion in which this software was used, including the version number, with a citation to the literature, in the *Methods* section, to allow replication; (b) mention this software in the *Acknowledgements* section. The appropriate citation is: Robert B. Laub (2003) "BLOBBER: A program that blobs", *Blobbing Bulletins* **12**(*34*):567-89. Moreover, as a personal note, I would appreciate it if you would email bobblaub@ubl.edu with citations of papers referencing this work so I can mention them to my funding agent and tenure committee.

h. **Q: Can I say "Users of this software must ..."?**

   A: Stop right there. Free software can't have *any* restrictions on use. (Under US copyright law it's not clear that it is even possible to restrict use, once someone has a legal copy.) We can only consider restrictions on distribution. So your license can't say "users must bathe regularly" or "users must tell me about particularly noteworthy uses" or "users must smile at someone who looks sad" or impose any usage condition whatsoever.

i. **Q: Can I say "You must not charge [much] money for distributing the program"?**

   A: This is non-free. We want Debian to be distributed by for-profit CD vendors and improved by corporate resellers. We can only include programs whose authors allow this.

   For many users buying Debian on disks is more convenient (and cheaper) than downloading. For-profit distribution is the most reliable and convenient way to ensure that Debian disks are easily available everywhere where there is a demand. Because everyone can download the CD images and start producing their own disks, competition ensures that nobody will make an undeserved fortune distributing Debian.

j. **Q: Can I say "You must not use the program for commercial purposes"?**

   A: This is non-free. We want businesses to be able to use Debian for their computing needs. A business should be able to use any program in Debian without checking its license.

k. **Q: Can I say "You must not change the program such that it**

does not implement what I say is the correct interface”?

A: This is non-free because it denies the user the freedom to adapt the software to a different problem which requires different interfaces.

We consider a very important facet of software freedom to be the freedom to adapt old tools to new problems. If I find a program in Debian which I think can be adapted to solve a problem I have (and which nobody ever thought about before), I expect to be allowed to make that adaptation---even if that means I need to change some of the external interfaces of the program. And I should not need to worry about the fact that my adapted tool does not solve the original problem anymore if the original problem is not what I need to solve.

Additionally: This kind of clause gives the author (authors are free to ignore their own rules) a *de facto* monopoly on experiments with alternative ways of doing things. It therefore fails the *Tentacles of Evil* test. One of the points of free software is that everyone should be free to try out new ways of doing things. This license clause denies the users the freedom to try out and exchange new ideas. This freedom is one of the most important driving factors for progress in computing---and we like progress.

l. **Q: Can I say “You must only distribute the program to people who have agreed to this license”?**

A: This is non-free because it makes it hard to mass distribute the program together with other programs, for example on an FTP site or CDs. Such clauses effectively forbid FTP distribution, and CD distribution would be prohibitively expensive and inconvenient if the CD manufacturer was required to make every customer sign a zillion different licenses. (See *clickwrap* above.)

m. **Q: Can I say “BY DOWNLOADING THIS SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE”?**

A: There are certain rights granted to anyone who is in lawful possession of a copy of a work, even when that work is under copyright. Free software gives you those rights (at least as they hold in the United States, where this is called *fair use*) plus a whole bunch more. Anything that tries to get the user to agree to “be bound by” something is almost certainly doing so in order to get them to agree to give up some of the rights they would otherwise automatically enjoy. After all, one does not need the user's agreement in order to *give* them extra rights. So boilerplate like the above is generally a promise that the license will, upon close examination, be found to contain something non-free. In other words, free software licenses do not *need* such an agreement.

n. **Q: Can I say "If you modify the program [and distribute your modifications] you must send your patch to me"?**

   A: This is non-free because it fails the *Desert Island* test and also the *Dissident* test.

o. **Q: Can I say "I reserve my right to withdraw your license if anyone claims they have copyright [or patent rights] to the program"?**

   A: This is non-free because (among other things) it fails the *Tentacles of Evil* test. However it would be okay to say "use of this software is at your own risk; this includes the risk of violating the patents or copyrights of third parties, which is the sole responsibility of the user and for which the software's authors are not responsible."

p. **Q: Can I say "You must obey U.S. export laws"?**

   A: This is non-free because it imposes restrictions on people outside the US which they might otherwise not be subject to. To protect yourself while keeping the license free you can rephrase this as a warning instead of a condition: "Please be aware that this license does not release you from your obligation to follow the law. We note in particular the US Export laws which may impact what you are legally allowed to do with this software, especially with regard to redistribution."

   A stronger way to phrase this is: It is not the job of a copyright license to reiterate what is or is not legal in a particular jurisdiction. *The job of a copyright license is to grant permissions to do things that would otherwise be forbidden under copyright law.*

q. **Q: Can I require users or distributors to check for updates using something like "You must monitor my website"? It is for their own protection.**

   A: This is non-free because it fails the *Desert Island* test. It is also an unreasonable burden---imagine if you had to constantly monitor 400 web sites in order to legally use the software on your computer.

r. **Q: I understand your logic, but my software is special and I'm really a very nice corporation and I have very innocuous and socially beneficial reasons for wanting to include a very small extra technically non-free clause that is in fact not so inconvenient as you seem to think. Plus this software was very expensive to develop, and is truly wonderful, and I'm trying very hard to contribute to the free software community in a way that is acceptable to my lawyers. Could you please make an**

exception just this once? You should at least compromise a little bit, because I have been very flexible on many other points.

A: No.

There are over 10,000 packages in Debian. If we made exceptions for just 1%, users would have to carefully evaluate how much of a burden the non-free parts of 100 licenses might be. It is simply not feasible, and we think we've drawn the line at the right place: where it is best for our users and for the free software community. (In any case, these matters are not subject to compromise. Think *satisfying the fire code* rather than *negotiating a deal*.)

As a bit of practical advice, you would really be better off using a standard license. It might be less fun for your lawyers, but your software will be more readily accepted, and more people will contribute to it. Isn't that what you want?

13. **Q: What does the DFSG mean by *no discrimination*? Doesn't the GPL discriminate against companies making proprietary software?**

    A: The intent is to prevent prohibitions against use by people fighting their own government, or building weapons of mass destruction, or Jews, or the French Postal Service. The DFSG contains a few more examples. The GPL does not discriminate against companies that want to make proprietary software based on GPLed code because they are given the same rights to GPLed software that anyone else has. They happen to also want the right to sell non-free derivative works, but no one is given that right so this does not constitute discrimination.

14. **Q: What about licenses that grant different rights to different groups? Isn't that discrimination, banned by DFSG#5/6?**

    A: For Debian's purposes, if all the different groups can exercise their DFSG rights, it is OK if there are other people who can do more. For example, if a work were distributed to everyone under the GPL, but elementary school teachers were given the extra right to distribute binaries without distributing the corresponding source code, it would still be DFSG-Free.

15. **Q: Since software “placed in the public domain” has no license isn't it not under a free software license, and therefore not acceptable as free software according to the DFSG?**

    A: Software placed in the public domain has all the freedoms required by the DFSG, and is free software.

16. **Q: The program FOO is free according to the DFSG and its license; can I now demand that Debian package FOO and include it in Debian GNU/Linux?**

    A: Although Debian includes *only* free software, we do not include *all* the free software in the whole world. (Although we do include so much that one can understand how people might think we include it all.) What software we choose to distribute is Debian's own decision, and no one else's. In particular, we are not obligated to distribute FOO.

    Here is what must occur for FOO to get into Debian GNU/Linux. First, it must be free, by *our* standards. Then it must be properly packaged, either by a Debian developer or by someone else. Then it must be *uploaded* to the Debian servers by a Debian developer. (This is called *sponsoring* if someone else actually did the packaging.) Then the Debian ftp masters must allow it in; they are a final screen against license issues or software integration problems. At this point the package is being distributed by Debian, but is not part of the official release. For that to occur it must be of sufficiently high quality to make it through a semi-automatic QA (Quality Assurance) process involving the Debian BTS, and the release manager must allow it to be included in the next major release.

    To initiate this process you can *file an RFP*. See Work-Needing and Prospective Packages for details.

17. **Q: What are *compatible licenses*, and what does *GPL compatible* mean?**

    A: In order for two licenses to be compatible it must be possible to mingle code under both licenses in a new work. When this is done the result is that the terms of both licenses must be met for the work as a whole. The GPL makes this feature of copyright law explicit by stating that if you cannot for any reason (e.g., because of another license) meet the terms of the GPL, the GPL grants no rights at all. In order for a license to be GPL compatible, then, you must be able to meet both the terms of the GPL and the other license simultaneously.

18. **Q: What is a *dual license*?**

    A: When a work is released under a *dual license* the recipient is explicitly given the option to choose which license to apply to a derivative work. Someone making modifications may include new code under either license, or (as is most common) under the same dual license.

19. **Q: Why in most dual licensed software is the GPL one of the licenses?**

    A: The GPL is particularly common in dual licenses because it allows the

code to link with the large body of GPLed code available including many important libraries, and to be incorporated into other GPLed works. Many common works are under dual GPL/xxx licenses: perl is under GPL/Artistic, Qt is under GPL/QPL, Mozilla is under GPL/MPL. This is almost always due to a project starting with a home-brewed GPL-incompatible license, then realizing they'd made a mistake and finding relicensing in this fashion to be the most convenient resolution.

20. **Q: Some programs distributed under the GPL read *"... under the ... GPL ... either version 2, or (at your option) any later version."* Others leave off the last clause, ending *"GPL version 2."* Why is this? Is code distributed "GPLv2 or later" compatible with code distributed under simply "GPLv2"?**

    A: This is an example of a dual license. Thus code distributed under "GPLv2 or later" can, at the redistributor's option, be redistributed instead under simply "GPLv2". A combined work containing both "GPLv2 or later" code and plain "GPLv2" code can only be redistributed under a plain "GPLv2".

    It is considered polite to retain the *"or later"* clause when a program using it is modified, if at all possible.

    The intent of the *"or later"* clause is to make a "license upgrade" easier, i.e. to allow the Free Software Foundation to fix any bugs or loopholes that might in the future be found in the GPLv2. Without this clause, moving a GPLv2 program to some future GPLv3 would require the permission of the copyright holders of all contributed code. This typically would include not just individuals but also their employers and former employers, some of whom may have gone through bankruptcy or mergers and had their assets, including copyrights, acquired by enormous multinationals or companies that specialize in liquidation. It can be very difficult to even find all the actual copyright holders and appropriate contact points, leave alone to explain the situation and convince them *all* to agree to a license change.

21. **Q: What is an *almost-free* license?**

    A: This is a license which seems written with the intent of making the software free, but with some problem that stymies this goal. Clauses like "only a reasonable fee may be charged for distribution" are typical; see above.

22. **Q: Do people really release programs under almost-free licenses?**

    A: Unfortunately yes. For instance iozone3, povray, or rar. Programs under almost-free licenses are typically, with time, either re-released under a free license (e.g., the Squeak Smalltalk system, or ckermit) or are replaced by superior free alternatives (e.g., xlock, superseded by the free

xscreensaver.)

23. **Q: What license does the Free Software Foundation (which sponsors the GNU project) advise?**

    A: The GPL. The FSF has declared the LGPL obsolete, and urges libraries to be released under the GPL unless there is a compelling reason to use the LGPL.

24. **Q: The FSF project asks for copyright assignments of all modifications submitted for inclusion in their projects. Does this put software at risk if the FSF should be acquired or infiltrated by a corporate enemy of free software, or lose a court battle and have its assets confiscated?**

    A: No. The FSF has clever lawyers who wrote the copyright assignment carefully to preclude any such danger.

25. **Q: What does *GNU LGPL* stand for?**

    A: The LGPL stands for Lesser General Public License. (It used to stand for Library General Public License, but no longer.)

26. **Q: Doesn't even Debian include some *non-free* software?**

    A: No.

    We do allow some non-free packages to use our distribution infrastructure, but they are not actually part of Debian proper. (There are some requirements on licenses for such non-free programs, so debian-legal does sometimes examine the licenses of non-free programs for distributability; it is not a priority though.) The existence of this non-free area can lead to confusion, so some members of Debian would like to remove non-free from our servers. On the other hand, many packages in non-free have migrated into Debian proper when their authors changed their almost-free licenses to make them actually free, and some have had their functionality painlessly migrated to newly available free alternatives. For this reason, other Debian developers want to retain the status quo.

27. **Q: What is the story with KDE and Debian and some license problem? I heard that Debian hates KDE.**

    A: KDE is currently in Debian. There is no license problem. We love KDE and always have, and included it in Debian the moment we were able to.

    Some time ago there was a license problem, but it has been resolved. The problem was that KDE was under the GPL while the Qt library, which it relied on, was under a rather odd license called the QPL, which although

(debatably) free was not GPL compatible. (And before that, Qt was under a license that didn't allow modifications at all.) This meant that Debian did not have permission to distribute KDE, at least as pre-compiled binaries, without a “Qt waiver” on all the KDE code, which we did not have. Debian was thus (very reluctantly) unable to distribute KDE. This license issue caused a fuss, and the result was (a) GNOME, and (b) TrollTech re-released the Qt library under a QPL/GPL dual license, which resolved the issue.

28. **Q: What is a *waiver* on a GPL-licensed program?**

    A: It is generally permission to create and distribute derived works that are linked to some particular library which is under a non-GPL-compatible license. For example, libssl is such a library and some GPLed programs use libssl. In order for such a program to be included in Debian, a note accompanying the license giving some extra permission must be present. Here is one such note (taken from /usr/share/doc/wget/copyright) which allows binaries of the GPLed program wget which are linked to the non-GPL-compatible OpenSSL library to be distributed:

    > In addition, as a special exception, the Free Software Foundation gives permission to link the code of its release of Wget with the OpenSSL project's "OpenSSL" library (or with modified versions of it that use the same license as the "OpenSSL" library), and distribute the linked executables. You must obey the GNU General Public License in all respects for all of the code used other than "OpenSSL". If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

29. **Q: If I release software under a free software license that does not allow others to make proprietary derived works, does this preclude me from making proprietary derived works myself?**

    A: No.

    Licenses gives *others* permissions that you already have. It is your code. You don't need your own permission to make a proprietary version, or to release a version under a different license, or to sell someone the right to make a proprietary version, or to sell someone the right to incorporate parts of your code in a proprietary program. (One caveat: if you incorporate non-trivial changes other people have made into your code base you are no longer the sole author. You would then need their permission to make a proprietary version, just as they would need yours.)

30. **Q: I want to release my code as free software, but am willing to allow people to pay for the right to include it in their proprietary programs. Should I say so in the license?**

We believe it is better (ie simpler and less confusing for everyone) to mention that in a separate note, rather than in the license. This allows you to use a standard free software license. It also tends to make the offer easier to see, since it would be buried if placed in a long document full of legalese.

31. **Q: What is the difference between *free software* and *open source software*?**

    A: There is no difference, or at least there isn't meant to be.

    “Open source software” was coined as a new name for “free software” which was intended to avoid the confusion arising from the fact that you're allowed to charge money for free software which can seem counterintuitive. It was also meant to give the community some branding power, because it was hoped that “open source software” could be controlled and legally permitted for use only on actual free software, whereas any company can distribute some proprietary software at no charge (eg Internet Explorer) and, since they are not charging any money, call it “free software”. (What we mean by the “free” in “free software” is of course a set of freedoms, not a price; “free as in free speech” rather than “free as in free beer”.) OSS was also meant to sound more professional and hence more attractive to businesses. In practice there are slight differences in emphasis between the people who use the two terms, and having two terms has caused confusion and a surprising amount of friction. Some people have begun to use terms like FLOSS (Free/Libre Open Source Software) to avoid both possible confusion and taking a side in the terminological debate.

    Some of the people who helped coin and popularize the term “open source software” have had second thoughts about it, and some of the legal measures originally planned (formal registration of the term “open source” as applied to software) did not actually come to fruition. The term “open source” is itself ambiguous, in that some companies “open” their source code for examination without granting the right to make changes or to pass on copies. The organization controlling the “open source software” certification mark made some borderline (ie controversial) determinations about some licenses, which served to dilute the standing of the mark itself.

    A number of people who made enormous contributions to Debian (eg Bruce Perens, former Debian project leader) and to free software in general have or held prominent positions in the Open Source Initiative. Nonetheless Debian in general, and this document in particular, uses the term “free software”. This is in part out of respect for the Free Software Foundation and the GNU project, in part to emphasize the large body of GNU code in Debian GNU/Linux, in part because the term “free software” seems more appropriate in technical forums because it sounds less corporate-speak,

and in part due to the issues discussed above.

32. **Q: What is the difference between *commercial* and *proprietary* software?**

    A: To quote the 1913 Webster's,

    > {*Proprietary articles*}, manufactured articles which some person or persons have exclusive right to make and sell.
    > --U. S. Statutes.
    >
    > {*Commercial*}. Of or pertaining to commerce; carrying on or occupied with commerce or trade; mercantile; as, commercial advantages; commercial relations. “Princely commercial houses.”
    > --Macaulay.

    Proprietary software is software that can be legally modified or distributed only by some authorized set of persons. So by definition *proprietary software* cannot be *free software*.

    Software is *commercial* if some corporation is distributing it and trying to make money from it, either via direct sales or via maintenance and support. Many corporations have made money by distributing, supporting, and maintaining free software, so it is possible for a piece of software to be both free and commercial. Anyone can sell a support contract for free software, and access to the source code allows such support to include not just hand-holding but also bug fixes and new features. This is a major advantage of free software as it makes for competition in such services, which is greatly to the benefit of users of free software. Corporations offering support contracts for free software include IBM, Redhat, LinuxCare, SAP, Trolltech, Ximbiot, and many others. Debian also encourages corporations to create products based on Debian GNU/Linux, such as Ubuntu. Many corporations pay employees to write and maintain free software from which they fully intend to make money, some of whom directly contribute their work to Debian as part of their jobs. Other employees of corporations are paid to maintain free software which is in internal use, and to contribute their modifications thus ensuring that their changes will not have to be re-applied to each new version.

33. **Q: If all software were free how could programmers make a living?**

    A: This question is extremely misleading. There is no reason to think that free software puts programmers in the poorhouse. In fact, the economics of the situation argue for quite the reverse! The vast majority of working computer programmers (over 95%) work at businesses that do not sell software: they write software for in-house use, for embedded devices, for driving new hardware, etc. Free software makes programmers more productive, which should have the effect of raising salaries. It also makes

programming more fun, since there is less need to re-invent the wheel. Moreover, even if free software reduced society's demand for programmers well below the current supply, so what? Automation and increased efficiency often reduce the number of jobs in some category and this is something we accept---buggy whip manufacturers come to mind---and Debian is not a trade union.

Debian itself takes no stand on the “morality” of proprietary software, or whether aspects of the current legal system which encourage proprietary software should be modified. Many people who write free software, including some Debian developers, also write proprietary software.

34. **Q: What are the FSF's *four freedoms*?**

    A: These four freedoms:

    - The freedom to run the program, for any purpose (freedom 0).
    - The freedom to study how the program works, and adapt it to your needs (freedom 1).
    - The freedom to redistribute copies so you can help your neighbor (freedom 2).
    - The freedom to improve the program, and release your improvements to the public, so that the whole community benefits (freedom 3).

    are the Free Software Foundation's articulation of what it believes all software users deserve. (Note that full exercise of Freedoms 1 and 3 requires access to the source code.) They are elegantly phrased, and arguably an improvement in some ways on the earlier DFSG. However they refer to exactly the same set of freedoms as the DFSG. If a license is inconsistent with the FSF's four freedoms, you can be sure that Debian will also consider it non-free.

    The term “four freedoms” is a play on words over the influential “four freedoms” speech of US President Franklin Delano Roosevelt in which he outlined the following four freedoms: Freedom of Speech, Freedom of Religion, Freedom from Want, and Freedom from Fear.

35. **Q: Why does Debian apply the DFSG to documentation?**

    A: Debian applies the same standards of freedom to all works it distributes; some of these standards are written down in the DFSG. No widely-accepted reasons have been provided to use different standards for documentation than for code.

    Even if we were to treat code and documentation differently, first we would need to have a clear way to tell documentation and code apart. Many works, like source code annotated with Javadoc comments or Postscript files, are programs and documentation at the same time, so it is very hard

to find such a clear division.

36. **Q: Shouldn't Debian allow documents which describe standards to be non-modifiable? Why should we need the same freedoms as for code?**

    A: We have three reasons: such a restriction is unnecessary; it is useless; and it is not true that it would be less appropriate for code than for documentation.

    First, misrepresentation can be prevented without forbidding anyone to modify the work, by requiring all modified works to not claim that they are the original work or that they were written by the original authors; so, the restriction is unnecessary.

    Furthermore, a clause in a copyright license would not prevent someone misrepresenting the work or its authors. For example, I might create a new, original document titled “RFC 2821, Simple Mail Transfer Protocol” with a distorted description of SMTP, and with this action I would not be contravening the license of the IETF's RFC 2821. The proper defense against this are the various laws dealing with libel, fraud and impersonation. So, such a restriction would be useless.

    Finally, if there were any reasons to allow such a restriction in documentation of standards, these reasons would allow it in programs too. For example, a standards document might be accompanied by a demonstration program. One could say that the reputations of the authors of the document and the program may suffer if someone breaks either one of them. If Debian allowed any restriction on modification of the document, Debian should also allow the same restriction on modification on the program, so this kind of restrictions would not be more appropriate for documentation than for programs.

37. **Q: Why isn't there a DFDG, “Debian Free Documentation Guidelines”, to complement the DFSG?**

    A: A number of people have proposed this idea, but have not met with any success to date. Serious consideration of adopting a DFDG entails someone actually writing one; this hurdle is surprisingly difficult. At that point, the obvious question that will be asked is why the proposed DFDG differs from the DFSG. In order to make a reasonable case, it seems necessary to justify each license restriction permitted by the proposed DFDG but not by the DFSG. Furthermore, it would be sensible to show how to distinguish which packages should be covered by the DFDG rather than the DFSG; why each particular restriction relaxed by the DFDG should be relaxed; and why they should be relaxed only for documentation but not for other software components, like code.

38. **Q: If the DFSG is to be applied to documentation as well as to programs, why is the text of the GPL included in Debian, if it says that it cannot be modified at all?**

    A: Because the verbatim text of the license must be distributed with any work licensed under its terms. This is not specific to the GPL; almost all free licenses require that their text be included verbatim with the work. As a compromise, Debian distributes copies of the GPL and other licenses under which the components of Debian are covered. This compromise will not be extended to other types of works.

    (Note that according to the FSF, which is the author of the GPL, you're actually allowed to modify the text of the GPL and create a derived license if you remove the preamble and you do not call the results “General Public License.” See the GNU GPL FAQ for more information.)

39. **Q: What FAQs remain to be added to this document?**

    A: What fraction of Debian packages/lines-of-code are under what licenses? What is an almost-free license (eg xlock's) and why should I avoid them? Some historical material, both summaries and pointers to longer treatments, would be nice. Some references. More links, both cross-references and references to other documents, would be useful.

40. **Q: Who wrote this document?**

    A: Barak A. Pearlmutter (bap@debian.org) with help from Joe Moore (joemoore@iegrec.org), Mark Rafn (dagon@dagon.net), Thomas Bushnell, BSG (tb@becket.net), Richard Braakman (dark@xs4all.nl), Henning Makholm (henning@makholm.net), Anthony Towns (aj@humbug.org.au), Jeremy Hankins (nowan@nowan.org), Florian Weimer (fw@deneb.enyo.de), Thomas Hood (jdthood@yahoo.co.uk), James Devenish (j-devenish@users.sourceforge.net), Glenn Maynard (glenn@zewt.org), Jacobo Tarrío (jtarrio@trasno.net), Andrew Suffield, Doug Jensen, Francesco Poli, Anthony DeRobertis, Raul Miller, Evan Prodromou, Ben Finney, Humberto Massa, MJ Ray.

Chapter 3

Containers, the GPL, and copyleft: No reason for concern (Richard Fontana)

Containers, the GPL, and copyleft: No reason for concern

Wondering how open source licensing affects Linux containers? Here's what you need to know.

24 Jan 2018 | Richard Fontana (Red Hat) (/users/fontana) | 246

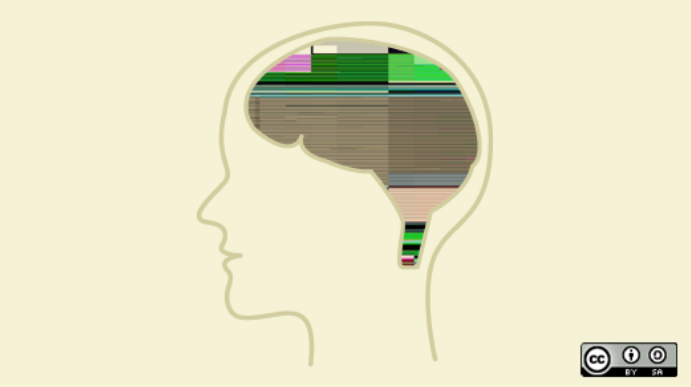


Image by : *Opensource.com*

Though open source is thoroughly mainstream, new software technologies and old

technologies that get newly popularized sometimes inspire hand-wringing about open source licenses. Most often the concern is about the GNU General Public License (GPL), and specifically the scope of its copyleft requirement, which is often described (somewhat misleadingly) as the GPL's derivative work issue.

One imperfect way of framing the question is whether GPL-licensed code, when combined in some sense with proprietary code, forms a single modified work such that the proprietary code could be interpreted as being subject to the terms of the GPL. While we haven't yet seen much of that concern directed to Linux containers, we expect more questions to be raised as adoption of containers continues to grow. But it's fairly straightforward to show that containers do *not* raise new or concerning GPL scope issues.

Statutes and case law provide little help in interpreting a license like the GPL. On the other hand, many of us give significant weight to the interpretive views of the Free Software Foundation (FSF), the drafter and steward of the GPL, even in the typical case where the FSF is not a copyright holder of the software at issue. In addition to being the author of the license text, the FSF has been engaged for many years in providing commentary and guidance on its licenses to the community. Its views have special credibility and influence based on its public interest mission and leadership in free software policy.

The FSF's existing guidance on GPL interpretation has relevance for understanding the effects of including GPL and non-GPL code in containers. The FSF has placed emphasis on the process boundary when considering copyleft scope, and on the mechanism and semantics of the communication between multiple software components to determine whether they are closely integrated enough to be considered a single program for GPL purposes. For example, the GNU Licenses FAQ (https://www.gnu.org/licenses/gpl-faq.en.html#MereAggregation) takes the view that pipes, sockets, and command-line arguments are mechanisms that are normally suggestive of separateness (in the absence of sufficiently "intimate" communications).

Consider the case of a container in which both GPL code and proprietary code might coexist and execute. A container is, in essence, an isolated userspace stack. In the OCI container image format (https://github.com/opencontainers/image-spec/blob/master/spec.md), code is packaged as a set of filesystem changeset layers, with the base layer normally being a stripped-down conventional Linux distribution without a

kernel. As with the userspace of non-containerized Linux distributions, these base layers invariably contain many GPL-licensed packages (both GPLv2 and GPLv3), as well as packages under licenses considered GPL-incompatible, and commonly function as a runtime for proprietary as well as open source applications. The "mere aggregation" clause (https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html#section2) in GPLv2 (as well as its counterpart GPLv3 provision on "aggregates" (https://www.gnu.org/licenses/gpl.html#section5)) shows that this type of combination is generally acceptable, is specifically contemplated under the GPL, and has no effect on the licensing of the two programs, assuming incompatibly licensed components are separate and independent.

Of course, in a given situation, the relationship between two components may not be "mere aggregation," but the same is true of software running in non-containerized userspace on a Linux system. There is nothing in the technical makeup of containers or container images that suggests a need to apply a special form of copyleft scope analysis.

It follows that when looking at the relationship between code running in a container and code running outside a container, the "separate and independent" criterion is almost certainly met. The code will run as separate processes, and the whole technical point of using containers is isolation from other software running on the system.

Now consider the case where two components, one GPL-licensed and one proprietary, are running in separate but potentially interacting containers, perhaps as part of an application designed with a microservices (https://www.redhat.com/en/topics/microservices) architecture. In the absence of very unusual facts, we should not expect to see copyleft scope extending across multiple containers. Separate containers involve separate processes. Communication between containers by way of network interfaces is analogous to such mechanisms as pipes and sockets, and a multi-container microservices scenario would seem to preclude what the FSF calls "intimate (https://www.gnu.org/licenses/gpl-faq.en.html#GPLPlugins)" communication by definition. The composition of an application using multiple containers may not be dispositive of the GPL scope issue, but it makes the technical boundaries between the components more apparent and provides a strong basis for arguing separateness. Here, too, there is no technical feature of containers that suggests application of a different and stricter approach to copyleft scope analysis.

A company that is overly concerned with the potential effects of distributing GPL-licensed code might attempt to prohibit its developers from adding any such code to a container image that it plans to distribute. Insofar as the aim is to avoid distributing code under the GPL, this is a dubious strategy. As noted above, the base layers of conventional container images will contain multiple GPL-licensed components. If the company pushes a container image to a registry, there is normally no way it can guarantee that this will not include the base layer, even if it is widely shared.

On the other hand, the company might decide to embrace containerization as a means of limiting copyleft scope issues by isolating GPL and proprietary code—though one would hope that technical benefits would drive the decision, rather than legal concerns likely based on unfounded anxiety about the GPL. While in a non-containerized setting the relationship between two interacting software components will often be mere aggregation, the evidence of separateness that containers provide may be comforting to those who worry about GPL scope.

Open source license compliance obligations may arise when sharing container images. But there's nothing technically different or unique about containers that changes the nature of these obligations or makes them harder to satisfy. With respect to copyleft scope, containerization should, if anything, ease the concerns of the extra-cautious.

Topics : **Licensing** (/tags/licensing) **Containers** (/tags/containers)

(/users/fontana)

About the author

Richard Fontana - Richard is Senior Commercial Counsel on the Products and Technologies team in Red Hat's legal department. Most of his work focuses on open source-related legal issues.

• More about me (/users/fontana)

- Learn how you can contribute (/participate)

Part II

Why Copyright Law Cannot Do Everything

Chapter 4

Hippocratic License (Coraline Ada Emkhe)

The Hippocratic License

Copyright (YEAR) (COPYRIGHT HOLDER)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

- The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

- The Software may not be used by individuals, corporations, governments, or other groups for systems or activities that actively and knowingly endanger, harm, or otherwise threaten the physical, mental, economic, or general well-being of individuals or groups in violation of the United Nations Universal Declaration of Human Rights (https://www.un.org/en/universal-declaration-human-

rights/).

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This license is derived from the MIT License, as amended to limit the impact of the unethical use of open source software.

OTHER FORMATS: MD TXT ADOC

The Hippocratic License was created by Coraline Ada Ehmke in 2019.

Support this and related initiatives through our Patreon or on Open Collective.

Chapter 5

Hacktivismo Enhanced-Source Software License Agreement (Oxblood Ruffin and Eric Grimm)

Hacktivismo

News About Projects

The Hacktivismo Enhanced-Source Software License Agreement

Everyone is permitted to copy and distribute verbatim copies of this license document. You may use content from this license document as source material for your own license agreement, but you may not use the name "Hacktivismo Enhanced-Source Software License Agreement ," ("HESSLA") or any confusingly similar name, trademark or service-mark, in connection with any license agreement that is not either (1) a verbatim copy of this License Agreement, or (2) a license agreement that contains only additional terms expressly permitted by The HESSLA.

INTRODUCTORY STATEMENT

Software that Hacktivismo[fn1] releases under this License Agreement is intended to promote our political objectives. And, likewise, the purpose of this License Agreement itself is political: Namely, to compliment the software's intended political function. Hacktivismo itself exists to develop and deploy computer software technologies that promote fundamental human rights of end-users. Hacktivismo also seeks to enlist the active participation and involvement of people around the world, to help us improve these software tools, and to take other actions (including actions that involve using and distributing our software, and the advancement of similarly-minded software projects of others) that promote human rights and freedom worldwide.

[fn1] http://hacktivismo.com/

Because of our non-commercial objective of promoting end-users' freedoms, Hacktivismo has some special, and admittedly ambitious, licensing needs. This License Agreement enhances the benefits of published source code by backing up our human rights projects with appropriate remedies enforceable in court.

The Freedoms We Promote: When we speak of the freedom of end-users, we are talking about basic freedoms recognized in the Hacktivismo Declaration,[fn2] the International Covenant on Civil and Political Rights,[fn3] the Universal Declaration of Human Rights,[fn4] and other documents that recognize and promote freedom and human dignity. Principal among these freedoms are:

[fn2] http://hacktivismo.com/about/declarations/

[fn3] http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

[fn4] http://www.un.org/Overview/rights.html

Freedom of Expression: The freedom of opinion and expression "include[s] freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers,"[fn5] and the freedom to choose one's own medium of expression. The arbitrary use of technological censorship measures to block or prevent access to broad categories of speech and expression including the work of critics, intellectuals, artists, journalists, and religious figures is seldom, if ever, justified by any legitimate governmental objective. And, to the extent that technology enables censorship decisions to be removed from public scrutiny and review, technology-based censorship mechanisms are especially suspect and dangerous to civil society. When repressive governments and other institutions of power seek to deprive people of this basic freedom, people have the right to secure, employ and deploy the tools necessary to reclaim the freedoms to which they are justifiably entitled.

[fn5] Article 19, Universal Declaration of Human Rights.

Freedom of Collective Action and Association: People have and should have the "freedom of peaceful assembly and association."[fn6] This freedom includes the right of people to work together to secure constructive change in their personal, economic, and political circumstances. When repressive governments or other institutions of power seek to deprive people (including users of the Internet) of their freedoms of voluntary assembly, association, and common enterprise, people have the right to secure, employ and deploy technologies that reclaim the freedoms to which they are justifiably entitled.

[fn6] Article 20(1), Universal Declaration of Human Rights.

Freedoms of Thought, Conscience, Sexuality, and Religion: People have and should have the freedom of "thought, conscience, and religion."[fn7] This right "includes freedom to change religion or belief, and freedom, either alone or in community with others, in public or private, to manifest any religion or belief in teaching, practice, worship and observance, regardless of doctrine."[fn8] Every person, regardless of sex or sexual preference, and with reciprocal respect for the corresponding rights of all others, has and should have the right to determine and choose, freely and without coercion, whether, how and with whom he or she shall fully enjoy the most private and personal aspects of human life, including individual sexuality, reproduction, and fertility. Moreover, "[t]he explicit recognition and reaffirmation of the right of all women to control all aspects of their health, in particular their own

fertility, is basic to their empowerment."[fn9] When repressive governments and other institutions of power seek to deprive people of these basic freedoms, they have the right to secure, employ and deploy the tools necessary to reclaim the freedoms to which they are justifiably entitled.

[fn7] Article 18, Universal Declaration of Human Rights.

[fn8] Id.

[fn9] Paragraph 17, Beijing Declaration of the Fourth United Nations Conference on Women (Sept. 15, 1995).

Freedom of Privacy: Every person has the right to be free from "subject[ion] to arbitrary interference with his [or her] privacy, family, home or correspondence"[fn10] -- digitally, or by any other means or methodology. This freedom of privacy includes the right to be free from governmental or private surveillance that might interfere with or deter the rightful exercise of any other freedoms of any person. In the context of software tools that enable people to reclaim their freedoms, all end-users have and should have the right to secure and use tools that are free from the surreptitious insertion into their software of "backdoors," "spy-ware," escrow mechanisms, or other code or techniques that might promote surveillance, or subvert security (including cryptographic security), confidentiality, anonymity, authenticity and/or trust.

[fn10] Article 12, Universal Declaration of Human Rights.

Reasons For Enhancing "Free" and "Open-Source" Licensing: Developing a new software license is never a trivial task and this License Agreement has presented special challenges for Hacktivismo. Because of our human rights objectives, this License Agreement includes some specific terms and conditions that, as a technical matter, depart from the previously-recognized and established definitions of "free"[fn11] software and "open source"[fn12] software.

[fn11] http://www.gnu.org/philosophy/free-sw.html

[fn12] http://www.opensource.org/docs/definition_plain.php

We have therefore coined the term "enhanced source" to describe this License Agreement because we have sought to combine most of the freedom-promoting benefits of "free" or "open-source" software (including mandatory disclosure of any changes or modifications Licensees make to the source code, whenever they release modified versions of HESSLA-licensed Programs or other Derivative Works), with additional enhanced license and contractual terms that are intended to promote the freedom of end-users. The Hacktivismo Enhanced-Source Software License Agreement promotes our objectives in an enhanced manner by including contractual terms that empower both Hacktivismo and qualified end-users with greater flexibility and leverage to maintain and recover human rights, through the mechanism of the contract itself including terms that are designed to enhance both our enforcement posture and that of qualified end-users in court.

To be sure, Hacktivismo enthusiastically endorses and supports the goals and objectives of the Free Software movement and those of the open source community. In particular, we owe a special debt of gratitude to the Free Software Foundation, to the Open Source Initiative, and to many exceedingly talented people who have contributed to Free Software and open source projects and endeavors over the years.

Ultimately, however, after reviewing the field of possibilities among previously-existing "open source" and "free" licenses, Hacktivismo has concluded that none of them fully meets our requirements. Writing our own License Agreement enables us to pursue our human rights objectives more effectively. This licensing endeavor represents a first step toward achieving our objectives, and no doubt informed feedback, scholarship, and learned commentary will enable us to pursue our objectives even more effectively in the future.

Benefits That Carry Over From Free Software: Before we explain how an "enhanced source" License Agreement specifically differs from a "free" or "open source" license, we believe it is helpful to explain in greater detail what the principal advantages, and freedom-enhancing aspects, of "free" software are.

When we speak of "free software," we refer to important personal freedoms, and not price. In addition to terms that are intended to promote the freedoms of Expression, Thought, Collective Action and Privacy (along with other human rights) of all end-users, the Hacktivismo Enhanced-Source Software License Agreement is also designed and intended to promote the following freedoms:

· You have the freedom to distribute copies of the software (and charge for this service if You wish);

· You have the freedom of access to the source code, to inspect and verify (and even to improve, if You can) the integrity and functionality of the software;

· So long as You do not subvert or infringe the freedoms of end-users by doing so, You have the freedom to change the software or to use parts of it in new Programs;

· You have the freedom to know You can do these things.

The licenses for most computer software programs are designed to take away Your freedom to share software or

change source code. This kind of software is designated as proprietary or "closed." The Hacktivismo Enhanced-Source Software License Agreement -- like other license agreements that have served as inspiration for our work -- is intended to promote both Your freedom to share our software with others, and Your freedom to change and improve the software. Your right under this License Agreement to look at the source not only enables You to contribute Your own efforts to Hacktivismo's human rights projects, but also serves as an additional level of assurance to You as an end-user that unwelcome, hidden surprises have not been inserted into the software, that could compromise Your rights and freedoms when You use the software.

HESSLA Helps Safeguard Additional End-User Freedoms: In order to understand why this License Agreement must be described as "enhanced source," and cannot strictly speaking be considered either a "free" or "open source" license agreement, it is helpful to consider the possibility that a programmer might insert malicious code, such as a computer virus, a keystroke logger, or "spyware" into a program that has previously been released under a "free software" license agreement.[fn13] The act of inserting malicious code into software, if done by a private individual or company (though many governments will contend they are not required to play by the same rules as the rest of us), may well violate criminal laws and result in civil tort liability. It is, of course, also possible to deter such malicious behavior by including, in a software license agreement, a specific contractual term that prohibits such behavior meaning that any licensee who violates the prohibition against malicious code can be sued by the licensor (or by third-party beneficiaries who the licensor has explicitly identified as alternate or additional enforcers of the agreement) for money damages and a court order forbidding any continued violation.

> [fn13]In this regard, a the following hypothetical illustration should be particularly helpful. If an organization of computer security enthusiasts were to release, under the GNU General Public License ("GPL"), a program called "Grey Eminence 3000" ("GE3K") a remote-administration tool for Microsoft Windows, that helps illustrate how insecure this particular commercial product happens to be it should hardly be surprising that the United States Secret Service and Federal Bureau of Investigation, after making some loud and misleading apocalyptic noises about "computer hackers" to Congress and in the media (primarily in a largely successful effort to increase their technology budgets), would also study the software to see what it does, how it does it, and whether any of those capabilities happen to be features that law enforcement might find helpful. Of course, if the U.S. federal law enforcement community were to announce, several months later, that it had commissioned the development of "classified" quasi-viral computer-intrusion and surveillance software called "Magic Candle" the capabilities of which law enforcement does not plan to disclose to the public, and the source code for which will remain a closely-guarded secret then inquiring minds might become curious as to whether "Magic Candle" contains any of the GPLed code that was written for "GE3K" (or any other free or open-source software, for that matter). Needless to say, under the right factual circumstances, if any GPLed code from GE3K found its way into "Magic Candle," then the U.S. government or its software development contractor might well be obligated to reveal to the public all the source code for "Magic Candle." Nevertheless, so long as the "Magic Candle" source is never publicly released for comparison purposes, then everyone with legitimate questions about GPL compliance faces a chicken-and-egg problem. So long as the source of "Magic Candle" remains secret, detection of a GPL violation becomes dramatically more difficult (particularly so if, additionally, nobody outside law enforcement has access to the compiled executables), which means the worldwide community of Internet users and software developers has only the United States government's solemn assurance that no GE3K code was used cold comfort at best.

Previous Licenses Provide More Limited Protection Against Government and Other Surveillance: No software license agreement that qualifies as "free" or "open source" may contain any restriction as a term of the license agreement that in any way qualifies any Licensee's prerogative (no matter who they are or what their motives may be) to make changes to code. In other words, an "open source" license agreement, to qualify for the "open source" label, may not even contain a term that prohibits the insertion of destructive viruses or "trojan horses" into derivative code. Likewise, no "free" or "open source" license agreement can in any way contain (as a license term) any restriction on the use of software not even a prohibition against unlawful surveillance or other malicious uses of the software.

The "open source" and "Free Software" communities rely principally on voluntary compliance[fn14] with the disclosure provisions of license agreements (although many "free" and "open source" license agreements, such as BSD-style licenses, do not require changed code to be disclosed, and in fact enable modified versions of programs to be "taken proprietary") and on social mechanisms of enforcement, as means to detect, prevent, deter, and remedy abuses.

> [fn14]As the example in Note 13 illustrates, it is sometimes difficult to determine whether the source disclosure requirement of the GPL has been violated, such as when a modified version of a program has been distributed without source, precisely because detection of a disclosure violation depends in part on the disclosure of the source of derivative works in order to compare whether a putative derivative really does contain code derived from a GPLed parent work.

The Hacktivismo Enhanced-Source Software License Agreement does not in any way sacrifice or surrender the enforcement techniques and safeguards available under license agreements such as the GNU General Public License. Rather, the HESSLA enhances the options available to Hacktivismo and to qualified end-users, by providing additional enforcement options. Moreover, for the purpose of promoting the freedoms of both programers and end-users, through the enforced mandatory disclosure of code modified by third-parties, this License

Agreement has advantages over many of the licenses (such as BSD-style licenses) that fully qualify as "free" or "open-source" license agreements.

What makes this License Agreement an "enhanced source" License Agreement, instead of a "free software" license agreement, is that the Hacktivismo Enhanced-Source Software License Agreement contains specific, very limited restrictions on modification and use of software by Licensees, as part of a calculated trade-off of rights and responsibilities that is intended to promote the freedom of end-users.

The Enhanced-Source Bargain Reinforces End-User Freedoms: To protect Your rights, we need to make restrictions that forbid anyone to deny You specific rights or to ask You to surrender these rights. To protect Your human rights as an end-user of this program or any work based on it, we need to make restrictions that forbid You and all other Licensees of this software (including, without limitation, any government Licensees) from using this code to subvert the human rights of any end-user.

We protect Your rights and the rights of all end-users with two steps: (1) copyright the software, and (2) offer You this License Agreement which gives You qualified legal permission to copy, distribute and/or modify the software.

The restrictions shared by all Licensees translate into certain responsibilities for You and for everyone else (including governmental entities everywhere) if You distribute copies of the software, if You use it, or if You modify it.

In this regard, the methodology we employ is not materially different from the methodology Free Software Foundation employs in the GNU General Public License (the "GPL"). The methodology is to exchange the Author's permission to copy, change, and/or distribute a copyrighted work, for every Licensee's acceptance of terms and conditions that promote the licensor's objectives. In both this License Agreement and the GPL, the terms and conditions that each Licensee must accept are intended to discriminate against certain very narrow, limited kinds of human endeavor, that are inconsistent with the licensor's political objectives. In other words, the GPL requires each Licensee to promise not to engage in the activity of 'propertizing,' or 'taking proprietary,' modifications to GPLed code; modified code must also be released under the GPL, and cannot be released in the form of "closed" executables, or otherwise be made "proprietary." Likewise, the Hacktivismo Enhanced Source Software License Agreement discriminates against undesirable activity such as surveillance, introduction of certain kinds of malicious code, and human rights violations, as well as discriminating against "propertizing" behavior such as might violate the GPL. Subject to these narrow restrictions, Licensees under either license agreement enjoy very broad latitude to change, use, explore, modify, and distribute the software much broader than they would enjoy with typical "proprietary" software packages.

As with "copyleft" licenses such as the GPL, under the Hacktivismo Enhanced Source Software License Agreement, programmers (including, most importantly, programmers working for governments) do not have unfettered or completely unlimited "freedom" for purposes of what they can do with HESSLA-licensed code. Just as with the GPL, they do not have the "freedom" to convert HESSLA-licensed code into "closed" or "proprietary" code. People who create derivative works based on an HESSLA-licensed program and distribute those works have a corresponding obligation to "give back," and not merely to "take," HESSLA-licensed code.

If You distribute copies of such an HESSLA-licensed program, whether gratis or for a fee, You must give the recipients all the rights and responsibilities that You have. You must ensure that they, too, are told of the terms of this License Agreement, including the freedoms they have, and the kinds of uses and modifications that are forbidden. You must communicate a copy of this License Agreement to them as part of any copy, modification, or re-use of source or object code, so they know their rights and responsibilities.

Thus, the main difference between this License Agreement and the GPL is not the methodology we employ,[fn15] but the scope and breadth of the political objectives we seek to promote. Simply put, the political objectives we promote are somewhat broader than the explicit political goals that the Free Software Foundation seeks to promote through the GPL. Our goals include a somewhat broader range of human rights than the specific copyright-related rights with which the GPL is principally concerned. But, while we are concerned with the entire field of human rights rather than a subset, we want to make it perfectly clear that we also embrace, share, and seek to promote, the goals we share with the Free Software movement.

> [fn15] There is a modest difference, but it is not large, and mostly philosophical. Some experts on the GPL draw a distinction between a "contract" and a pure "license," by taking the position that a pure "license" does not impose "contractual" conditions on a Licensee only conditions that would otherwise (but for the license) be subsumed within with exclusive rights that the licensor has under copyright law. Thus, the licensor has the right to exclude anyone else from such activities as making copies, making derivative works, publicly performing a work, and other exclusive rights specified by statute. But, concerning the act of "using" a computer software program, in instances in which a copy is not made (or, in the trivial sense that a copy is made only temporarily from a storage medium to memory, to enable software to be "used"), the Free Software Foundation takes the position that United States law, at least, does not confer an exclusive right on the copyright holder (or, as others would argue, the United States statute qualifies the holder's exclusive right to copy),because the U.S. Copyright Act specifically exempts from the exclusive right to make copies, a copy made from (for example) a computer hard drive to volatile memory, in connection with the process of executing computer software. So far as we can determine, the Free Software Foundation does not argue that it is impossible "contractually" to impose conditions on use, as part of the bargain one strikes, when conditionally allowing Licensees to make copies of a program. Rather, for philosophical reasons, the Free Software Foundation voluntarily chooses not

> to include what it views as "contractual" conditions in the GPL. In this sense, Hactivismo takes the position that the HESSLA is clearly a "contract" and contains "contractual" terms, such that it should not be considered a "pure license," under the nomenclature employed by the Free Software Foundation. However, in our view, precisely because both the HESSLA and the GPL are clearly conditional grants of permission to do things from which the Licensee would otherwise be excluded (i.e., the Licensee must undertake certain obligations in exchange for permission to copy, modify, or distribute, a work), the key point is that the methodology is quite similar.

Compared with the GPL, aspects of the HESSLA give both end-users and programmers (including, most importantly, governmental end-users and programmers) marginally less leeway to make malicious use of the program, or to insert malicious code into a program, than they would have under a traditional "copyleft" software license. These aspects of the HESSLA (such as the requirement that the program cannot be used to violate human rights, or forbidding the insertion of "spy-ware" or surveillance mechanisms into derivative works) are included because our ultimate objective is to preserve and promote the human rights of end-users, including their privacy and their right of free expression.

In other words, unlike many programmers, we are not just in the business of developing and distributing open-standards technologies. We're also trying to empower end-users (including end-users in totalitarian regimes) with software tools that promote fundamental freedoms while also seeking as best we can to protect these end-users from being arrested, beaten, or worse. Our objective of promoting end-user freedoms, including the freedoms of people in politically repressive countries, is precisely the factor that has led Hacktivismo to develop this License Agreement instead of using another.

The HESSLA Also Includes Features To Enhance Government Accountability: To this end, we have sought and intend to ensure, to the fullest extent that law (including, without limitation, the law of contract and of copyright licensing) enables us to do so,[fn16] that no government or other institution may do anything with this computer software or the underlying source code without becoming a Licensee bound by the terms of this License Agreement, subject to the same restrictions on modification and use as anyone else.

> [fn16] "Everyone has the right to an effective remedy by the competent national tribunals for acts violating . . . fundamental rights . . ." Article 8, United Nations Declaration of Human Rights.

Accordingly, this License Agreement includes several terms that are aimed explicitly at governmental entities, in order to maximize enforceability against such entities. Respect for the Rule of Law means that no governmental entity is above the law, and that no governmental entity should be permitted to use its status as a mechanism for circumventing the requirements of this License Agreement.

Any use, copying or modification of this software by any governmental official or governmental entity anywhere in the world is a voluntary act, which act the governmental official or entity is free to forego if it does not wish to be bound by this License Agreement. This License Agreement seeks to establish as clearly as possible two important checks on the improper use of government power. First, the voluntary election to use, copy, or modify, this software by any government or governmental official constitutes a waiver of all immunities that might otherwise be asserted, against enforcement of this License Agreement by the Author, or assertion by end-users or others of any human rights laws that may have been violated by a government employing the Software. Second, any such government or governmental official not only subjects itself to enforcement action in its own courts, but also explicitly and voluntarily subjects itself to enforcement action in the courts of other nations that are likely to be more objective, for the purpose of giving effect to the terms of this License Agreement.

Mechanism of Contract Acceptance: This License Agreement treats any use of the software as acceptance of the terms of this License Agreement. To understand the significance of this, it is important to distinguish between the law governing copyright and the law governing offer and acceptance for the purpose of contract formation (which gives the offeror the power to specify the manner of acceptance). The question of whether copyright confers an exclusive right of use on the author of a program is certainly an interesting one. Under United States law, see 17 U.S.C. 117(a)(1), a limited exception to the exclusive right to copy exists if one makes a second copy "created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner." This License Agreement presupposes that there is no exclusive right to use in the Copyright Act, just an exclusive right to copy. However, You may not make a copy for anyone else unless they are subject to the terms of this License Agreement. Nor may You permit anyone to use Your copy or any other copy You have made unless they are subject to the terms of this License Agreement. You may not make a copy for Your own use or the use of anyone else without the Author's leave to make that copy. And any use, modification, copying, or distribution by anyone constitutes acceptance of the License Agreement, for purposes of contract law. In other words, the License Agreement is designed so that there is no loophole permitting anyone to claim the ability to use, copy, distribute, or modify the Program or any Software based on it without subjecting themselves voluntarily to its terms.

On "Shrinkwrap," "Click-Wrap," "Use-Wrap" and "Copy-Wrap" License Agreements: Arguably, some kinds of software license agreements have more in common with legislation than they do with the bargained-for, negotiated agreements that come to mind when most people think of "contracts." Particularly if a software licensor has sufficient market power to be deemed a monopoly, or if certain proposed expansions of the law of software licensing, masquerading as "codifications," are widely adopted, the ability of a private entity to impose legal prohibitions and duties on virtually everyone else as though the licensor has assumed powers that customarily belong to legislative bodies is both breathtaking and deeply troubling. Of course, we are hardly the first to distribute software under a license agreement that imposes conditions on a take-it-or-leave-it basis. This technique is, as everyone knows, extremely common with proprietary software. And some of the conditions unilaterally imposed by

proprietary licensors range from the ridiculous to the obscene. But even certain kinds of "free" and "open-source" software licenses, such as the GPL, depend on the continued viability of legal rules that enable at least some reasonable conditions to be imposed by software licensors on a take-it-or-leave-it basis, with essentially automated methods of acceptance. Courts have been divided as to how far these kinds of licensor-driven automated agreements can go. And we cannot say that we will be unhappy if courts or legislatures ultimately reach a consensus that sharply limits what conditions licensors can impose through such mechanisms. However, while the law is still developing, we think nothing could be more appropriate than to enlist the techniques that institutions of power have used to limit freedom and instead to re-purpose the techniques of "copy-wrap" or "use-wrap" licensing by putting them to use for humanitarian purposes and using them to promote the human rights of end-users. To deny us the use of these techniques, courts and other law-making institutions would be required simultaneously to disarm, to the same degree, proprietary software manufacturers that possess vast market power. And, unlike the conditions imposed by many proprietary vendors, the conditions we impose through this License Agreement are hardly onerous for any end-user (unless, of course, the end-user wants to act maliciously or engage in surveillance).

No Warranty: Next, for each author's protection and our own, we want to make certain that everyone understands that there is no warranty for this software. And, if the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Software Patents: Software patents constantly threaten any project such as this one. We wish to avoid the danger that redistributors of a HESSLA-licensed program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have included terms by which any Author must, if it has patented (or licensed a patent covering) any technology embodied in any Program or Software released under this License Agreement, grant all HESSLA Licensees of the Program or Software a royalty-free license of that technology. Any Licensees who release derivative works, as permitted by this License Agreement, are required to grant a royalty-free patent license of any patented technology.

Anyone Can Release Original Software Under The HESSLA: Although this License Agreement is drafted with Hacktivismo's objectives in mind, perhaps it will meet other authors' needs as well. If You are considering using this License Agreement for Your own software (meaning the code is not a work based on Hacktivismo's program in which case all derivative works must be released under this License Agreement but rather Your code is original software that You have developed yourself) and if You have no special reason to prefer this License Agreement to some license that has a more robust and widely-understood track-record, then in most instances we encourage You to use the GPL (or, even better, release concurrently under both the HESSLA and the GPL), because a considerable body of interpretive literature and community custom has grown up around that License Agreement. The Open Software License, see < http://www.rosenlaw.com/osl.html >, is newer and has less of a track record. But You may also want to consider that licensing option (as well as the option of concurrent OSL/HESSLA licensing).

Any author of original software can release that software under this License Agreement, if You choose to do so; not just Hacktivismo. Hacktivismo is the author and owner of software released by Hacktivismo under this License Agreement. But original software released by other Authors would be owned and licensed by them.

Ultimately, we think it is important to emphasize to other Authors that Programs they have written can be released under both the HESSLA and some other license simultaneously (for, example, a program that is presently GPLed by its Author can be released simultaneously under both the GPL and the HESSLA, at the Author's discretion). If You are an Author of original work, You need neither the permission of the Free Software Foundation nor of Hacktivismo to elect to release software simultaneously under both licenses. The advantage of such a voluntary double-licensing is that it will enable developers to produce hybrid software packages (combining the functionality available through, say, Hacktivismo's Six-Four APIs, with some of the functionality of one or more popular GPL-licensed communications programs) and to release the hybrid packages under the HESSLA, without causing those developers to run afoul of the GPL, the HESSLA or both. Such an arrangement maximizes the potential benefit to both the developer community and to end-users worldwide. Software released under a BSD-style license, as a general matter, can be used to produce a hybrid program, mixing HESSLA-licensed code with code that was previously subject to a BSD license. The HESSLA requires that, in such an instance, the hybrid code must be released under the HESSLA (to avoid weakening the end-user protections and affirmative rights afforded by the HESSLA). Hacktivismo is more than happy to consult with any software developer about the license terms that should apply to any Software that is derivative of any Program of which Hacktivismo is Author. If another Author has released code under the HESSLA, then that Author has primary decision-making authority about the manner in which his her or its software is licensed, but Hacktivismo is happy to field any questions hat may be posed by such an Author or by any developer who is building on another Author's HESSLAed code.

License Revisions: This License Agreement is subject to revision, prior to the release of the Hacktivismo Enhanced-Source Software License Agreement, Version 1.0. We invite interested parties from the international academic and legal communities to offer comments and suggestions on ways to improve this License Agreement, prior to the time that The HESSLA version 1.0 is released.

The terms of the latest and most up-to-date version of this License Agreement, up to and including version 1.0, shall be deemed automatically to supersede the terms of any lower-numbered version of this License Agreement with respect to any Licensee who became a Licensee under the lower-numbered version of the HESSLA.

The terms of the latest and most up-to-date version of this License Agreement will always be published on the Hacktivismo Website, http://www.hacktivismo.com/.

The precise terms and conditions for copying, distribution, use and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION, USE AND/OR MODIFICATION

0. DEFINITIONS. The following are defined terms that, whenever used in this License Agreement, have the following meanings:

0.1 Author: "Author" shall mean the copyright holder of an Original Work (the "Program") released by the Author under this License Agreement.

0.2 Copy: "Copy" shall mean everything and anything that constitutes a copy according to copyright law, without limitation. A "copy" does not become anything other than a "copy" merely because, for example, a governmental or institutional employee duplicates the Program or a part of it for another employee of the same institution or Governmental Entity, or merely because it is copied from one computer to another, or from one medium to another, or multiple copies are made on the same medium, within the same institutional or Governmental Entity.

0.3 Derivative Work: A "Derivative Work" or "work based on the Program" shall mean either the Program itself or any work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification."). In the unlikely event that, and to the extent that, this contractual definition of "Derivative Work" is later determined by any tribunal or dispute-resolution body to be different is scope from the meaning of "derivative work" under the copyright law of any country, then the broadest and most encompassing possible definition either the contractual definition of "Derivative Work," or any broader and more encompassing statutory or legal definition, shall control. Acceptance of this contractually-defined scope of the term "Derivative Work" is a mandatory pre-condition for You to receive any of the benefits offered by this License Agreement.

0.3.1 Mere aggregation of another work not based on the Program with the Program (or with a Derivative Work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License Agreement.

0.4 License Agreement: When used in this License Agreement, the terms "this License" or "this License Agreement" shall mean The Hactivismo Enhanced-Source Software License Agreement, v. 0.1, or any subsequent version made applicable under the terms of Section 15.

0.5 Licensee: The term "Licensee" shall mean You or any other Licensee, whether or not a Qualified Licensee.

0.6 Original Work: "Original Work" shall mean a Program or other work of authorship, or portion thereof, that is not a Derivative Work.

0.7 Program: The "Program," to which this License Agreement applies, is the Original Work (including, but not limited to, computer software) released by the Author under this License Agreement.

0.8 Qualified Licensee: A "Qualified Licensee" means a Licensee that remains in full compliance with all terms and conditions of this License Agreement. You are no longer a Qualified Licensee if, at any time, You violate any terms of this License Agreement. Neither the Program nor any Software based on the Program may be copied, distributed, performed, displayed, used or modified by You, even for Your own purposes, unless You are a Qualified Licensee. A Licensee other than a Qualified Licensee remains subject to all terms and conditions of this License Agreement, and to all remedies for each cumulative violation as set forth herein. Loss of the status of Qualified Licensee signifies that violation of any terms of the License Agreement subjects a Licensee to loss of most of the benefits that Qualified Licensees enjoy under this License Agreement, and to additional remedies for all violations occurring after the first violation.

0.9 Software: "Software" or "the Software" shall mean the Program, any Derivative Work based on the Program or a portion thereof, and/or any modified version of the Program or portion thereof, without limitation.

0.10 Source Code: The term "Source Code" shall mean the preferred form of a Program or Original Work for making modifications to it and all available documentation describing how to access and modify that Program or Original Work.

0.10.1 For an executable work, complete Source Code means all the Source Code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the Source Code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

0.10.2 "Object Code:" Because of certain peculiarities of current export-control rules, "object code" of the Program, or any modified version of the Program, or Derivative Work based on the Program, must not be exported except by way of distribution that is ancillary to the distribution of the Source Code. The "Source Code" shall be understood as the primary content transferred or exported by You, and the "object code" shall be considered as merely an ancillary component of any such export distribution.

0.11 Strong Cryptography: "Strong Cryptography" shall mean cryptography no less secure than (for example, and without limitation) a 2048-bit minimum key size for RSA encryption, 1024-bit minimum key size for Diffie-Hellman (El Gamal), or a 256-bit minimum key size for AES and similar symmetric ciphers.

0.12 Substandard Key-Selection Technique: The term "Substandard Key-Selection Technique" shall mean a

method or technique to cause encryption keys to be more easily guessed or less secure, such as by (i) causing the selection of keys to be less than random, or (ii) employing a selection process that selects among only a subset of possible keys, instead of from among the largest set of possible keys that can securely be used consistent with contemporary knowledge about the cryptographic techniques employed by You. The following illustrations elaborate on the foregoing definition:

0.12.1 If the key-generation or key-selection technique for the encryption algorithm You employ involves the selection of one or more prime numbers, or involves one or more mathematical functions or concatenations performed on one or more prime numbers, then each prime number should be selected from a very large set of candidate prime numbers, but not necessarily from the set of all possible prime numbers (e.g., inclusion of the number 1 in the candidate set, for example, may in some instances reduce rather than enhance security), and absolutely not from any artificially small set of candidate primes that makes the guessing of a key easier than would be the case if a secure key-generation technique were employed. In all instances, the primes should be selected at random from among the candidate set. If there is a customary industry standard for maximizing the security associated with the key-generation or key-selection technique for the cryptosystem You select, then (with attention also to the requirements of Section 0.11), You should employ a key-generation or selection technique no less secure than the customary industry standard for secure use of the cryptosystem.

0.12.2 If the key-generation or key-selection technique for the encryption algorithm You employ involves the selection of a random integer, or the transformation of a random integer through one or more mathematical processes, then the selection of the integer shall be at random from the largest possible set of all possible integers consistent with the secure functioning of the encryption algorithm. It shall not be selected from an artificially small set of integers (e.g., if a 256-bit random integer serves as the key, then You could not set 200 of the 256 bits as "0," and randomly generate only the remaining 56 bits producing effectively a 56-bit keylength instead of using the full 256 bits).

0.12.3 In other words, Your key-generation technique must promote security to the maximum extent permitted by the cryptographic method(s) and keylength You elect to employ, rather than facilitating eavesdropping or surveillance in any way. The example of GSM telephones, in which 16 of 56 bits in each encryption key were set at "0," thereby reducing the security of the system by a factor of 65,536, is particularly salient. Such artificial techniques to reduce the security of a cryptosystem by selecting keys from only a less-secure or suboptimal subset of possible keys, is prohibited and will violate this License Agreement if any such technique is employed in any Software.

0.13 You: Each Licensee (including, without limitation, Licensees that have violated the License Agreement and who are no longer Qualified Licensees, but who nevertheless remain subject to all requirements of this License Agreement and to all cumulative remedies for each successive violation), is referred to as "You."

0.13.1 Governmental Entity: "You" explicitly includes any and all "Governmental Entities," without limitation. "Governmental Entity" or "Governmental Entities," when used in this License Agreement, shall mean national governments, sub-national governments (for example, and without limitation, provincial, state, regional, local and municipal governments, autonomous governing units, special districts, and other such entities), governmental subunits (without limitation, governmental agencies, offices, departments, government corporations, and the like), supra-national governmental entities such as the European Union, and entities through which one or more governments perform governmental functions or exercise governmental power in coordination, cooperation or unison.

0.13.2 Governmental Person: "You" also explicitly includes "Governmental Persons." The terms "Governmental Person" or "Governmental Persons," when used in this License Agreement, shall mean the officials, officers, employees, representatives, contractors and agents of any Governmental Entity.

1. Application of License Agreement. This License Agreement applies to any Program or other Original Work of authorship that contains a notice placed by the Author saying it may be distributed under the terms of this License Agreement. The preferred manner of placing such a notice is to include the following statement immediately after the copyright notice for such an Original Work:

"Licensed under the Hacktivismo Enhanced-Source Software License Agreement, Version 0.1"

2. Means of Acceptance Use, Copying, Distribution or Modification By Anyone Constitutes Acceptance. Subject to Section 14.1 (concerning the special case of certain Governmental Entities) any copying, modification, distribution, or use by You of the Program or any Software, shall constitute Your acceptance of all terms and conditions of this License Agreement.

2.1 As a Licensee, You may not authorize, permit, or enable any person to use the Program or any Software or Derivative Work based on it (including any use of Your copy or copies of the Program) unless such person has accepted this License Agreement and has become a Licensee subject to all its terms and conditions.

2.2 You may not make any copy for Your own use unless You have accepted this License Agreement and subjected yourself to all its terms and conditions.

2.3 You may not make a copy for the use of any other person, or transfer a copy to any other person, unless such person is a Licensee that has accepted this License Agreement and such person is subject to all terms and conditions of this License Agreement.

2.4 It is not the position of Hacktivismo that copyright law confers an exclusive right to use, as opposed to the exclusive right to copy the Software. However, for purposes of contract law, any use of the Software shall be considered to constitute acceptance of this License Agreement. Moreover, all copying is prohibited unless the recipient of a copy has accepted the License Agreement. Because each such recipient Licensee is contractually obligated not to permit anyone to access, use, or secure a copy of the Software, without first accepting the terms and conditions of this License Agreement, use by non-Licensees is effectively prohibited contractually because nobody can obtain a copy of, or access to a copy of, any Software without (1) accepting the License Agreement through use, and (2) triggering some Licensee's obligation to require acceptance as a precondition of copying or access.

3. "Qualified Licensee" Requirement: Neither the Program nor any Software or Derivative Work based on the Program may be copied, distributed, displayed, performed, used or modified by You, even for Your own purposes, unless You are a "Qualified Licensee." To remain a Qualified Licensee, You must remain in full compliance with all terms and conditions of this License Agreement.

4. License Agreement Is Exclusive Source of All Your Rights:

4.1 You may not copy, modify, or distribute the Program, or obtain any copy, except as expressly provided under this License Agreement. Any attempt otherwise to copy, modify, obtain a copy, sublicense or distribute the Program is void, and will automatically terminate Your rights under this License Agreement and subject You to all cumulative remedies for each successive violation that may be available to the Author. However, Qualified Licensees who have received copies from You (and thereby have received rights from the Author) under this License Agreement, and who would otherwise qualify as Qualified Licensees, will not have their rights under their License Agreements suspended or restricted on account of anything You do, so long as such parties remain in full compliance.

4.2 You are not required to accept this License Agreement and prior to the time You elect to become a Licensee and accept this License Agreement, You may always elect instead not to copy, use, modify, distribute, compile, or perform the Program or any Software released under this License Agreement. However, nothing else grants You permission to copy, to obtain or possess a copy, to compile a copy in object code or executable code from a copy in source code, to modify, or to distribute the Program or any Software based on the Program. These actions are prohibited by law if You do not accept this License Agreement. Additionally, as set forth in Section 2, any use, copying or modification of the Software constitutes acceptance of this License Agreement by You.

4.3 Each time You redistribute the Program (or any Software or Derivative Work based on the Program), the recipient automatically receives a License Agreement from the Author to copy, distribute, modify, perform or display the Software, subject to the terms and conditions of this License Agreement. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License Agreement. Enforcement is the responsibility of the Author.

5. Grant of Source Code License.

5.1 Source Code Always Available from Author: Author hereby promises and agrees except to the extent prohibited by export-control law to provide a machine-readable copy of the Source Code of the Program at the request of any Licensee. Author reserves the right to satisfy this obligation by placing a machine-readable copy of the Source Code of the most current version of the Program in an information repository reasonably calculated to permit inexpensive and convenient access by You for so long as Author continues to distribute the Program, and by publishing the address of that information repository in a notice immediately following the copyright notice that applies to the Program. Every copy of the Program distributed by Hacktivismo (but not necessarily every other Author) consists of the Source Code accompanied, in some instances, by an ancillary distribution of compiled Object Code, but the continued availability of the Source Code from the Author addresses the possibility that You might have (for any reason) not received from someone else a complete, current, copy of the Source Code (lack of which would, for example, prevent You from exporting copies to others without violating this license, see Section 8).

5.2 Grant of License. If and only if, and for so long as You remain a Qualified Licensee, in accordance with Section 3 of this License Agreement, Author hereby grants You a world-wide, royalty-free, non-exclusive, non-sublicensable copyright license to do the following:

5.2.1 to reproduce the Source Code of the Program in copies;

5.2.2 to prepare Derivative Works based upon the Program and to edit or modify the Source Code in the process of preparing such Derivative Works;

5.2.3 to distribute copies of the Source Code of the Original Work and/or of Derivative Works to others, with the proviso that copies of Original Work or Derivative Works that You distribute shall be licensed under this License Agreement, and that You shall fully inform all recipients of the terms of this License Agreement.

6. Grant of Copyright License. If and only if, and for so long as You remain a Qualified Licensee, in accordance with Section 3 of this License Agreement, Author hereby grants You a world-wide, royalty-free, non-exclusive, non-sublicensable license to do the following:

6.1 to reproduce the Program in copies;

6.2 to prepare Derivative Works based upon the Program, or upon Software that itself is based on the Program;

6.3 to distribute (either by distributing the Source Code, or by distributing compiled Object Code, but any export of

Object Code must be ancillary to a distribution of Source Code) copies of the Program and Derivative Works to others, with the proviso that copies of the Program or Derivative Works that You distribute shall be licensed under this License Agreement, that You shall fully inform all recipients of the terms of this License Agreement;

6.4 to perform the Program or a Derivative Work publicly;

6.5 to display the Program or a Derivative Work publicly; and

6.6 to charge a fee for the physical act of transferring a copy of the Program (You may also, at Your option, offer warranty protection in exchange for a fee).

7. Grant of Patent License. If and only if, and for so long as You remain a Qualified Licensee, in accordance with Section 3 of this License Agreement, Author hereby grants You a world-wide, royalty-free, non-exclusive, non-sublicensable license Agreement, under patent claims owned or controlled by the Author that are embodied in the Program as furnished by the Author ("Licensed Claims") to make, use, sell and offer for sale the Program. Subject to the proviso that You grant all Licensees a world-wide, non-exclusive, royalty-free license under any patent claims embodied in any Derivative Work furnished by You, Author hereby grants You a world-wide, royalty-free, non-exclusive, non-sublicensable license under the Licensed Claims to make, use, sell and offer for sale Derivative Works.

8. Exclusions From License Agreement Grants. Nothing in this License Agreement shall be deemed to grant any rights to trademarks, copyrights, patents, trade secrets or any other intellectual property of Licensor except as expressly stated herein. No patent license is granted to make, use, sell or offer to sell embodiments of any patent claims other than the Licensed Claims defined in Section 7. No right is granted to the trademarks of Author even if such marks are included in the Program. Nothing in this License Agreement shall be interpreted to prohibit Author from licensing under additional or different terms from this License Agreement any Original Work, Program, or Derivative Work that Author otherwise would have a right to License.

8.1 Implied Endorsements Prohibited. Neither the name of the Author (in the case of Programs and Original Works released by Hacktivismo, the name "Hacktivismo"), nor the names of contributors who helped produce the Program may be used to endorse or promote modifications of the Program, any Derivative Work, or any Software other than the Program, without specific prior written permission of the Author. Neither the name of Hacktivismo nor the names of any contributors who helped write the Program may be used to endorse or promote any Program or Software released under this License Agreement by any person other than Hacktivismo.

9. Modifications and Derivative Works. Only Qualified Licensees may modify the Software or prepare or distribute Derivative Works. If You are a Qualified Licensee, Your authorization to modify the Software or prepare or distribute Derivative Works (including permission to prepare and/or distribute Derivative Works, as provided in Sections 5.2.2, 5.2.3, 6.2, 6.3, and 6.6) is subject to each and all of the following mandatory terms and conditions (9.1 through 9.6, inclusive):

9.1 You must cause the modified files to carry prominent notices stating that You changed the files and the date of any change;

9.2 If the modified Software normally reads commands interactively when run, You must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that You provide a warranty) and that users may redistribute the program under this License Agreement, and telling the user how to view a copy of this License Agreement. (Exception: if the Program itself is interactive but does not normally print such an announcement, Your Derivative Work based on the Program is not required to print an announcement.);

9.3 Any Program, Software, or modification thereof copied or distributed by You, that incorporates any portion of the Original Work, must not contain any code or functionality that subverts the security of the Software or the end-user's expectations of privacy, anonymity, confidentiality, authenticity, and trust, including (without limitation) any code or functionality that introduces any "backdoor," escrow mechanism, "spy-ware," or surveillance techniques or methods into any such Program, Software, or modification thereof;

9.4 Any Program, Software, or modification thereof copied or distributed by You, that employs any cryptographic or other security, privacy, confidentiality, authenticity, and/or trust methods or techniques, including without limitation any Derivative Work that includes any changes or modifications to any cryptographic techniques in the Program, shall employ Strong Cryptography.

9.5 Any Program, Software, or modification thereof copied or distributed by You, if it contains any key-generation or selection technique, must not employ any Substandard Key-Selection Technique.

9.6 No Program or Software copied or distributed by You may transmit or communicate any symmetric key, any "private key" if an asymmetric cryptosystem is employed, or any part of such key, nor may it otherwise make any such key or part of such key known, to any person other than the end-user who generated the key, without the active consent and participation of that individual end-user. If a private or symmetric key is stored or recorded in any manner, it must not be stored or recorded in plaintext, and it must be protected from reading (at a minimum) by use of a password. Use of steganography or other techniques to disguise the fact that a private or symmetric key is even stored is strongly encouraged, but not absolutely required.

10. Use Restrictions: Human Rights Violations Prohibited.

10.1 Neither the Program, nor any Software or Derivative Work based on the Program may used by You for any of

the following purposes (10.1.1 through 10.1.5, inclusive):

10.1.1 to violate or infringe any human rights or to deprive any person of human rights, including, without limitation, rights of privacy, security, collective action, expression, political freedom, due process of law, and individual conscience;

10.1.2 to gather evidence against any person to be used to deprive any person of human rights;

10.1.3 any other use as a part of any project or activity to deprive any person of human rights, including not only the above-listed rights, but also rights of physical security, liberty from physical restraint or incarceration, freedom from slavery, freedom from torture, freedom to take part in government, either directly or through lawfully elected representatives, and/or freedom from self-incrimination;

10.1.4 any surveillance, espionage, or monitoring of individuals, whether done by a Governmental Entity, a Governmental Person, or by any non-governmental person or entity;

10.1.5 censorship or "filtering" of any published information or expression.

10.2 Additionally, the Program, any modification of it, or any Software or Derivative Work based on the Program may not be used by any Governmental Entity or other institution that has any policy or practice (whether official or unofficial) of violating the human rights of any persons.

10.3 You may not authorize, permit, or enable any person (including, without limitation, any Governmental Entity or Governmental Person) to use the Program or any Software or Derivative Work based on it (including any use of Your copy or copies of the Program) unless such person has accepted this License Agreement and has become a Licensee subject to all its terms and conditions, including (without limitation) the use restrictions embodied in Section 10.1 and 10.2, inclusive.

11. All Export Distributions Must Consist of or Be Ancillary to Distribution of Source Code. Because of certain peculiarities of current export-control law, any distribution by You of the Program or any Software may be in the form of Source Code only, or in the form or Source Code accompanied by compiled Object Code, but You may not export any Software in the form of compiled Object Code only. Such an export distribution of compiled executable code must in all cases be ancillary to a distribution of the complete corresponding machine-readable source code, which must be distributed on a medium, or by a method, customarily used for software interchange.

12. EXPORT LAWS: THIS LICENSE AGREEMENT ADDS NO RESTRICTIONS TO THE EXPORT LAWS OF YOUR JURISDICTION. It is Your responsibility to comply with any export regulations applicable in Your jurisdiction. From the United States, Canada, or many countries in Europe, export or transmission of this Software to certain embargoed destinations (including, but not necessarily limited to, Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria), may be prohibited. If Hacktivismo is identified as the Author of the Program (and it is not the property of some other Author), then export to any national of Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria, or into the territory of any of these countries, by any Licensee who has received this Software directly from Hacktivismo or from the Cult of the Dead Cow, or any of their members, is contractually prohibited and will constitute a violation of this License Agreement. You are advised to consult the current laws of any and all countries whose laws may apply to You, before exporting this Software to any destination. Special care should be taken to avoid export to any embargoed destination. An Author other than Hacktivismo may substitute that Author's legal name for "Hacktivismo" in this Paragraph, in relation to any Program released by that Author under this Paragraph.

13. Contrary Judgments, Settlements and Court Orders. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on You (whether by court order, agreement or otherwise) that contradict the conditions of this License Agreement, they do not excuse You from the conditions of this License Agreement. If You cannot distribute so as to satisfy simultaneously Your obligations under this License Agreement and any other pertinent obligations, then as a consequence You may not distribute the Software at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through You, then the only way You could satisfy both it and this License Agreement would be to refrain entirely from distribution of the Program.

It is not the purpose of this Section 13 to induce You to infringe any patents or other property right claims or to contest validity of any such claims; this Section has the sole purpose of protecting the integrity of the software distribution system reflected in this License Agreement, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through related distribution systems, in reliance on consistent application of such distribution systems; it is up to the Author/donor to decide if he or she is willing to distribute software through any other system and a Licensee cannot impose that choice.

14. Governmental Entities: Any Governmental Entity ("Governmental Entity" is defined broadly as set forth in Section 0.13.1) or Governmental Person (as "Governmental Person" is defined broadly in Section 0.13.2), that uses, modifies, changes, copies, displays, performs, or distributes the Program, or any Software or Derivative Work based on the Program, may do so if and only if all of the following terms and conditions (14.1 through 14.10, inclusive) are agreed to and fully met:

14.1 If it is the position of any Governmental Entity (or, in the case of any "Governmental Person," if it is the position of that Governmental Person's Governmental Entity) that any doctrine or doctrines of law (including, without limitation, any doctrine(s) of immunity or any formalities of contract formation) may render this License Agreement unenforceable or less than fully enforceable against such Governmental Entity, or any Governmental Person of such Governmental Entity, then prior to any use, modification, change, display, performance, copy or

distribution of the Program, or of any Software or Derivative Work based on the Program, or any part thereof, by the Governmental Entity, or by any Governmental Person of that Governmental Entity, the Governmental Entity shall be required to inform the Author in writing of each such doctrine that is believed to render this License Agreement or any part of it less than fully enforceable against such Governmental Entity or any Governmental Person of such entity, and to explain in reasonable detail what additional steps, if taken, would render the License Agreement fully enforceable against such entity or person. Failure to provide the required written notice to the Author in advance of any such use, modification, change, display, performance, copy or distribution, shall constitute an irrevocable and conclusive waiver of any and all reliance on any doctrine, by the Governmental Entity, that is not included or that is omitted from the required written notice (failure to provide any written notice means all reliance on any doctrine is irrevocably waived). Any Governmental Entity that provides written notice under this subsection is prohibited, as are all of the Governmental Persons of such Governmental Entity, from making any use, change, display, performance, copy, modification or distribution of the Software or any part thereof, until such time as a License Agreement is in place, agreed upon by the Author and by the Governmental Entity, that such entity concedes is fully-enforceable. Any use, modification, change, display, performance, copy, or distribution following written notice under this Paragraph, but without the implementation of an agreement as provided herein, shall constitute an irrevocable and conclusive waiver by the Governmental Entity (and any and all Governmental Persons of such Governmental Entity) of any and all reliance on any legal doctrine either referenced in such written notice or omitted from it.

14.2 Any Governmental Entity that uses, copies, changes, modifies, or distributes, the Software or any part or portion thereof, or any Governmental Person who does so (whether that person's Governmental Entity contends the person's action was, or was not, authorized or official), permanently and irrevocably waives any defense based on sovereign immunity, official immunity, the Act of State Doctrine, or any other form of immunity, that might otherwise apply as a defense to, or a bar against, any legal action based on the terms of this License Agreement.

14.2.1 With respect to any enforcement action brought by the Author in a United States court against a foreign Governmental Entity, the waiver by any Governmental Entity as provided in Subparagraphs 14.1 and 14.2 is hereby expressly acknowledged by each such Governmental Entity to constitute a "case . . . in which the foreign state has waived its immunity," within the scope of 28 U.S.C. 1605(a)(1) of the Foreign Sovereign Immunities Act of 1976 (as amended). Each such Governmental Entity also specifically agrees and concedes that the "commercial activity" exceptions to the FSIA, 28 U.S.C. 1605(a)(2), (3) are also applicable. With respect to an action brought against the United States or any United States Governmental Entity, in the courts of any country, the U.S. Governmental Entity shall be understood to have voluntarily agreed to a corresponding waiver of immunity from actions in the courts of any other sovereign.

14.2.2 With respect to any enforcement action brought by an authorized end-user (as a third-party beneficiary, under the terms of Subparagraphs 14.3 and 14.10) in a United States court against a foreign Governmental Entity, the waiver by any Governmental Entity as provided in Subparagraphs 14.1 and 14.2 is hereby expressly acknowledged by each such Governmental Entity to constitute a "case . . . in which the foreign state has waived its immunity," within the scope of 28 U.S.C. 1605(a)(1) of the Foreign Sovereign Immunities Act of 1976 (as amended). . Each such Governmental Entity also specifically agrees and concedes that the "commercial activity" exceptions to the FSIA, 28 U.S.C. 1605(a)(2), (3) are also applicable. With respect to an action brought against the United States or any United States Governmental Entity, in the courts of any country, the U.S. Governmental Entity shall be understood to have voluntarily agreed to a corresponding waiver of immunity from actions in the courts of any other sovereign.

14.2.3 With respect to any action or effort by the Author in the United States to execute a judgment against a foreign Governmental Entity, by attaching or executing process against the property of such Governmental Entity, the waiver by any Governmental Entity as provided in Subparagraphs 14.1 and 14.2 is hereby expressly acknowledged by each such Governmental Entity to constitute a case in which "the foreign state has waived its immunity from attachment in aid of execution or from execution," in accordance with 28 U.S.C. 1610(a)(1) of the Foreign Sovereign Immunities Act of 1976 (as amended). Each such Governmental Entity also specifically agrees and concedes that the "commercial activity" exceptions to the FSIA, 28 U.S.C. 1610(a)(2), (d) are also applicable. With respect to an action brought against the United States or any United States Governmental Entity, in the courts of any country, the U.S. Governmental Entity shall be understood to have voluntarily agreed to a corresponding waiver of immunity from actions in the courts of any other sovereign.

14.2.4 With respect to any action or effort brought by an authorized end-user (as a third-party beneficiary, in accordance with Subparagraphs 14.3 and 14.10) in the United States to execute a judgment against a foreign Governmental Entity, by attaching or executing process against the property of such Governmental Entity, the waiver by any Governmental Entity as provided in Subparagraphs 14.1 and 14.2 is hereby expressly acknowledged by each such Governmental Entity to constitute a case in which "the foreign state has waived its immunity from attachment in aid of execution or from execution," in accordance with 28 U.S.C. 1610(a)(1) of the Foreign Sovereign Immunities Act of 1976 (as amended). Each such Governmental Entity also specifically agrees and concedes that the "commercial activity" exceptions to the FSIA, 28 U.S.C. 1610(a)(2), (d) are also applicable. With respect to an action brought against the United States or any United States Governmental Entity, in the courts of any country, the U.S. Governmental Entity shall be understood to have voluntarily agreed to a corresponding waiver of immunity from actions in the courts of any other sovereign.

14.3 Any Governmental Entity that uses, copies, changes, modifies, displays, performs, or distributes the Software or any part thereof, or any Governmental Person who does so (whether that person's Governmental Entity contends the person's action was, or was not, authorized or official), and thereby violates any terms and conditions of Section 9 (restrictions on modification), or Paragraph 10 (use restrictions), agrees that the person or entity is subject not only to an action by the Author, for the enforcement of this License Agreement and for money damages

and injunctive relief (as well as attorneys' fees, additional and statutory damages, and other remedies as provided by law), but such Governmental Entity and/or Person also shall be subject to a suit for money damages and injunctive relief by any person whose human rights have been violated or infringed, in violation of this License Agreement, or through the use of any Software in violation of this License Agreement. Any person who brings an action under this section against any Governmental Person or Entity must notify the Author promptly of the action and provide the Author the opportunity to intervene to assert the Author's own rights. Damages in such a third-party action shall be measured by the severity of the human rights violation and the copyright infringement or License Agreement violation, combined, and not merely by reference to the copyright infringement. All end-users, to the extent that they are entitled to bring suit against such Governmental Entity by way of this License Agreement, are intended third-party beneficiaries of this License Agreement. Punitive damages may be awarded in such a third-party action against a Governmental Entity or Governmental Person, and each and every such Governmental Entity or Person conclusively waives all restrictions on the amount of punitive damages, and all defenses to the award of punitive damages to the extend such limitations or defenses depend upon or are a function of such person or entity's status as a Governmental Person or Governmental Entity.

14.4 Any State of the United States, or any subunit or Governmental Entity thereof, that uses, copies, changes, modifies, displays, performs, or distributes the Software of any part thereof, or any of whose Governmental Persons does so (whether that person's Governmental Entity contends the person's action was, or was not, authorized or official), unconditionally and irrevocably waives for purposes of any legal action (i) to enforce this License Agreement, (ii) to remedy infringement of the Author's copyright, or (iii) to invoke any of the third-party beneficiary rights set forth in Section 14.3 -- any immunity under the Eleventh Amendment of the United States Constitution or any other immunity doctrine (such as sovereign immunity or qualified, or other, official immunity) that may apply to state governments, subunits, or to their Governmental Persons.

14.5 Any Governmental Entity (including, without limitation, any State of the United States), that uses, copies, changes, modifies, performs, displays, or distributes the Software or any part thereof, or any of whose Governmental Persons does so (whether that person's Governmental Entity contends the person's action was, or was not, authorized or official), unconditionally and irrevocably waives for purposes of any legal action (i) to enforce this License Agreement, (ii) to remedy infringement of the Author's copyright, or (iii) to invoke any of the third-party beneficiary rights set forth in Section 14.3 any doctrine (such as, but not limited to, the holding in the United States Supreme Court decision of Ex Parte Young) that might purport to limit remedies solely to prospective injunctive relief. Also explicitly and irrevocably waived is any underlying immunity doctrine that would require the recognition of such a limited exception for purposes of remedies. The remedies against such governmental entities and persons shall explicitly include money damages, additional damages, statutory damages, consequential damages, exemplary damages, punitive damages, costs and fees that might otherwise be barred or limited in amount on account of governmental status.

14.6 Any Governmental Entity that uses, copies, changes, modifies, displays, performs, or distributes the Software or any part thereof, or any of whose Governmental Persons does so (whether that person's Governmental Entity contends the person's action was, or was not, authorized or official), unconditionally and irrevocably waives for purposes of any legal action (i) to enforce this License Agreement, (ii) to remedy infringement of the Author's copyright, or (iii) to invoke any of the third-party beneficiary rights set forth in Section 14.3 any and all reliance on the Act of State doctrine, sovereign immunity, international comity, or any other doctrine of immunity whether such doctrine is recognized in that government's own courts, or in the courts of any other government or nation.

14.6.1 Consistent with Subparagraphs 14.2.1 through 14.2.4, this waiver shall explicitly be understood to constitute a waiver not only against suit, but also against execution against property, for purposes of the Foreign Sovereign Immunities Act of 1976 (as amended). All United States Governmental Entities shall be understood to have agreed to a corresponding waiver of immunity against (i) suit in the courts of other sovereigns, and (ii) execution against property of the United States located within the territory of other countries.

14.7 Governmental Persons, (i) who violate this License Agreement (whether that person's Governmental Entity contends the person's action was, or was not, authorized or official), or (ii) who are personally involved in any activity, policy or practice of a governmental entity that violates this License Agreement (whether that person's Governmental Entity contends the person's action was, or was not, authorized or official), or (iii) that use, copy, change, modify, perform, display or distribute, the Software or any part thereof, when their Governmental Entity is not permitted to do so, or is not a Qualified Licensee, or has violated the terms of this License Agreement, each and all individually waive and shall not be permitted to assert any defense of official immunity, "good faith" immunity, qualified immunity, absolute immunity, or other immunity based on his or her governmental status.

14.8 No Governmental Entity, nor any Governmental Person thereof may, by legislative, regulatory, or other action, exempt such Governmental Entity, subunit, or person, from the terms of this License Agreement, if the Governmental Entity or any such person has voluntarily used, modified, copied, displayed, performed, or distributed the Software or any part thereof.

14.9 Enforcement In Courts of Other Sovereigns Permitted. By using, modifying, changing, displaying, performing or distributing any Software covered by this License Agreement, any Governmental Entity hereby voluntarily and irrevocably consents, for purposes of (i) any action to enforce the terms of this License Agreement, and (ii) any action to enforce the Author's copyright (whether such suit be for injunctive relief, damages, or both) to the jurisdiction of any court or tribunal in any other country (or a court of competent jurisdiction of a subunit, province, or state of such country) in which the terms of this License Agreement are believed by the Author to be enforceable. Each such Governmental Entity hereby waives all objections to personal jurisdiction, all objections based on international comity, all objections based on the doctrine of forum non conveniens, and all objections based on sovereign or governmental status or immunity that might otherwise be asserted in the courts of some

other sovereign.

14.9.1 The Waiver by any Governmental Entity of a country other than the United States shall be understood explicitly to constitute a waiver for purposes of the Foreign Sovereign Immunities Act of 1976 (see Subparagraphs 14.2.1to 14.2.4, inclusive, supra), and all United States Governmental Entities shall be understood to have agreed to a waive correspondingly broad in scope with respect to actions brought in the courts of other sovereigns.

14.9.2 Forum Selection Non-U.S. Governmental Entities. Governmental Entities that are not United States Governmental Entities shall be subject to suit, and agree to be subject to suit, in the United States District Court for the District of Columbia. The Author or an authorized end-user may bring an action in another court in another country, but the United States District Court for the District of Columbia, shall always be available as an agreed-upon forum for such an action. At the optional election of any Author (or, in the case of a third-party claim, any end-user asserting rights under Subparagraphs 14.3 and 14.10), such a suit against a non-U.S. Governmental Entity or Person may be brought in the United States District Court for the Southern District of New York, or the United States District Court for the Northern District of California, as a direct substitute for the United States District Court for the District of Columbia, for all purposes of this Subparagraph.

14.9.3 Forum Selection U.S. Governmental Entities. All United States Governmental Entities shall be subject to suit, and agree to be subject to suit, in the following (non-exclusive) list of fora: Ottawa, Canada, London, England, and Paris, France. The Author or an authorized end-user may bring action in another court that can exercise jurisdiction. But the courts in these three locations shall always be available (at the option of the Author or an authorized end-user) as a forum for resolving any dispute with the United States or a governmental subunit thereof. Except as provided in Subparagraph 14.10, any and all United States Governmental Persons shall be subject to suit wherever applicable rules of personal jurisdiction and venue shall permit such suit to be filed, but no such United States Governmental Person may assert any defense based on forum non conveniens or international comity, to the selection of any particular lawful venue.

14.10 Enforcement Of Claims For Human Rights Violations. By using, copying, modifying, changing, performing, displaying or distributing the Software covered by this License Agreement, any Governmental Entity, or Governmental Person hereby voluntarily and irrevocably consents -- for purposes of any third-party action to remedy human rights violations and other violations of this License Agreement (as reflected in Section 14.3) -- to the jurisdiction of any court or tribunal in any other country (or a court of competent jurisdiction of a subunit, province, or state of such country) in which the third-party beneficiary reasonably believes the relevant terms of this License Agreement are enforceable. The Governmental Entity or Person hereby waives all objections to personal jurisdiction, all objections based on international comity, all objections based on the doctrine of forum non conveniens, and all objections based on sovereign or governmental status or immunity that might otherwise be asserted in the courts of some other sovereign.

14.10.1 Waiver of Immunity and Forum Selection. The presumptively valid and preferred fora identified in Subparagraphs 14.9.2 and 14.9.3 shall also apply for purposes of Subparagraph 14.10. All Governmental Entities are subject to the same Waiver of Immunity as set forth in Subparagraphs 14.2.1 to 14.2.4, inclusive.

15. Subsequent Versions of HESSLA. Hacktivismo may publish revised and/or new versions of the Hacktivismo Enhanced-Source Software License Agreement from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. Any Program released by Hacktivismo under a version of this License Agreement prior to Version 1.0, shall be considered released under Version 1.0 of the Hacktivismo Enhanced-Source Software License Agreement, once Version 1.0 is formally released. Prior to Version 1.0, any Software released by Hacktivismo or a Licensee of Hacktivismo under a lower-numbered version of the HESSLA shall be considered automatically to be subject to a higher-number version of the HESSLA, whenever a later-numbered version has been released.

Concerning the work of any other Author, if the Program specifies a version number of this License Agreement which applies to it and "any later version," You have the option of following the terms and conditions either of that version or of any later version published by Hacktivismo. If the Program does not specify a version number of this License Agreement, You may choose any version after 1.0, once version 1.0 is published by Hacktivismo, and prior to publication of version 1.0, You may choose any version of the Hacktivismo Software License Agreement then published by Hacktivismo. If the Program released by another Author, specifies only a version number, then that version number only shall apply. If "the latest version," is specified, then the latest version of the HESSLA published on the Hacktivismo Website shall always apply at all times.

16. DISCLAIMER OF WARRANTY. THE SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF NON-INFRINGEMENT AND WARRANTIES THAT THE ORIGINAL WORK IS MERCHANTABLE OR FIT FOR A PARTICULAR PURPOSE. THE SOFTWARE IS PROVIDED WITH ALL FAULTS. THE ENTIRE RISK AS TO THE QUALITY OF THE ORIGINAL WORK IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO LICENSE TO ORIGINAL WORK IS GRANTED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

17. LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING THE AUTHOR'S NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL THE AUTHOR BE LIABLE TO ANY PERSON FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER ARISING AS A RESULT OF THIS LICENSE OR THE USE OF THE

SOFTWARE INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PERSON SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION, BUT SHALL EXCLUDE SUCH LIABILITY TO THE EXTENT PERMITTED BY LAW. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

18. ENCRYPTION KEYS AND PUBLIC KEY INFRASTRUCTURE. SOFTWARE RELEASED UNDER THIS LICENSE AGREEMENT MAY REQUIRE A DIGITAL CERTIFICATE, OR AN ENCRYPTION KEY "SIGNED" BY A TRUSTED PARTY, TO FUNCTION. AUTHOR UNDERTAKES NO RESPONSIBILITY FOR THE PROPER, SECURE, AND ADEQUATE FUNCTIONING OF ANY CRYPTOGRAPHIC SYSTEMS, OF ANY CRYPTOGRAPHIC KEYS, OR FOR THE TRUSTWORTHINESS OF ANY END-USER, ANY ISSUER OF CERTIFICATES, OR OF ANY SIGNER OF ENCRYPTION KEYS. USE OF THIS SOFTWARE IS AT THE END-USER'S SOLE AND EXCLUSIVE RISK. IN ANY PUBLIC-KEY INFRASTRUCTURE ("PKI") SYSTEM, AN END-USER'S LEGAL RELATIONSHIP WITH THE END-USER'S CERTIFICATION AUTHORITY DOES NOT INCLUDE OR ENCOMPASS ANY LEGAL RELATIONSHIP WITH THE AUTHOR, AND IS GOVERNED SOLELY AND EXCLUSIVELY BY THE CERTIFICATION AUTHORITY'S CERTIFICATION PRACTICE STATEMENT AND CERTIFICATION AGREEMENTS. AUTHOR ASSUMES NO RESPONSIBILITY FOR THE ACTIONS OR OMISSIONS OF ANY END-USER OR ANY CERTIFICATION AUTHORITY.

18. Saving Clause. If any portion of this License Agreement is held invalid or unenforceable under any particular circumstance, the balance of the License Agreement is intended to apply and the License Agreement as a whole is intended to apply in other circumstances.

END OF TERMS AND CONDITIONS

Chapter 6

Anti-996 License (Katt Gu)

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS
FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT
HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN ANY WAY CONNECTION
WITH THE LICENSED WORK OR THE USE OR OTHER DEALINGS IN THE LICENSED WORK.

Chapter 7

MongoDB Server Side Public License

mongoDB.

Server Side Public License FAQ

Table of Contents

- What will happen if someone in the community is currently building something on MongoDB Community Server?
- How does this affect customers who use MongoDB as a service from cloud providers today?

Why are we changing the license for MongoDB?

Back to Table of Contents

The market is quickly moving to consume most software as a service. This is a time of incredible opportunity for open source projects, with the potential to foster a new wave of great open source server side software. The reality, however, is that once an open source project becomes interesting, it is too easy for large cloud vendors to capture all the value but contribute nothing back to the community.

Given this risk, small companies are unwilling to make that bet, so most software being written is closed source.

We believe an open development approach leads to more valuable, robust and secure software, and it directly enables a stronger community and better products.

The community needs a new license that builds on the spirit of the AGPL, but makes explicit the conditions for providing the software as a service.

As an example, MongoDB has become one of the most popular databases in the industry. As a result, we have observed organizations, especially the international cloud vendors begin to test the boundaries of the AGPL license.

Rather than litigating this issue in the courts, we are issuing a new license to eliminate any confusion about the specific conditions of offering a publicly available MongoDB as a service.

This change is also designed to make sure that companies who do run a publicly

It should be noted that the new license maintains all of the same freedoms the community has always had with MongoDB under AGPL - they are free to use, review, modify, and redistribute the source code. The only changes are additional terms that make explicit the conditions for offering a publicly available MongoDB as a service.

Obviously, this new license helps our business, but it is also important for the MongoDB community. MongoDB has invested over $300M in R&D over the past decade to offer an open database for everyone, and with this change, MongoDB will continue to be able to aggressively invest in R&D to drive further innovation and value for the community.

What is the new license called and what will be licensed under it?

Back to Table of Contents

The new license is called the Server Side Public License (SSPL). All MongoDB Community Server patch releases and versions released on or after October 16, 2018, will be subject to this new license, including future patch releases of older versions.

Are you basing the SSPL on an OSI-recognized open source license?

Back to Table of Contents

Yes, we have based the SSPL on the GNU General Public License, version 3, but it is a new license introduced by MongoDB, not the Free Software Foundation. The SSPL has not been approved by the OSI.

the GPL and the SSPL?

Back to Table of Contents

1. The only substantive modification is section 13, which makes clear the condition to offering MongoDB as a service. A company that offers a publicly available MongoDB as a service must release the software it uses to offer such service under the terms of the SSPL, including the management software, user interfaces, application program interfaces, automation software, monitoring software, backup software, storage software and hosting software, all such that a user could run an instance of the service using the source code made available.

Section 13 of the SSPL reads as follows:

a.
"If you make the functionality of the Program or a modified version available to third parties as a service, you must make the Service Source Code available via network download to everyone at no charge, under the terms of this License. Making the functionality of the Program or modified version available to third parties as a service includes, without limitation, enabling third parties to interact with the functionality of the Program or modified version remotely through a computer network, offering a service the value of which entirely or primarily derives from the value of the Program or modified version, or offering a service that accomplishes for users the primary purpose of the Software or modified version."

b.
"Service Source Code" means the Corresponding Source for the Program or the modified version, and the Corresponding Source for all programs that you use to make the Program or modified version available as a service, including, without limitation, management software, user interfaces, application program interfaces, automation software, monitoring software, backup software, storage software and hosting software, all such that a user could run an instance of the service using the Service Source Code you make available."

A full copy of the SSPL is here.

Why did you base the SSPL on GPL v3

Back to Table of Contents

The AGPL is a modified version of GPL v3. The only additional requirement of AGPL is in section 13: if you run a modified program on a server and let other users communicate with it there, you must open source the source code corresponding to your modified version, known as the "Remote Network Interaction" provision of AGPL.

There is some confusion in the marketplace about the trigger and scope of the Remote Network Interaction provision of AGPL.

As a result, we decided to base the SSPL on GPL v3 and to add a new section 13 which clearly and explicitly sets forth the conditions to offering the licensed program as a third-party service.

Does section 13 of the SSPL apply if I'm offering MongoDB as a service for internal-only use?

Back to Table of Contents

No. We do not consider providing MongoDB as a service internally or to subsidiary companies to be making it available to a third party.

Will MongoDB continue to provide open source software?

Back to Table of Contents

Yes, MongoDB supported drivers and connectors such as the MongoDB Connector for

All versions of MongoDB Community Server released prior to October 16, 2018 will continue to be licensed under the Free Software Foundation's GNU AGPL v3.0.

Although the SSPL is not OSI approved, it maintains all of the same freedoms the community has always had with MongoDB under AGPL. Users are free to review, modify, and distribute the software or redistribute modifications to the software. However, the Open Source Initiative (OSI) has its own process for approving what it considers to be an open source license, and the SSPL has not received OSI approval. MongoDB software licensed under the SSPL is not considered open source by the OSI.

Will you let others use the new license? Can they use it on their own?

Back to Table of Contents

Yes, anyone can adopt this license, and we hope that many organizations and individuals will use it to protect themselves, their communities, and their intellectual property.

How does the license change the current usage of MongoDB Community Server? Are those users grandfathered in?

Back to Table of Contents

All versions of MongoDB's Community Server released on or after October 16, 2018, including patch fixes for prior versions, will be licensed under the SSPL. Prior versions of MongoDB Community Server released before October 16th, 2018 will remain under the AGPL; therefore, any use of those versions is governed by AGPL.

What are the implications of this new license on applications built using MongoDB and made available as a service (SaaS)?

Back to Table of Contents

The copyleft condition of Section 13 of the SSPL applies only when you are offering the functionality of MongoDB, or modified versions of MongoDB, to third parties as a service. There is no copyleft condition for other SaaS applications that use MongoDB as a database.

What are the implications of this new license on your customers and partners?

Back to Table of Contents

This SSPL will apply to MongoDB Community Server. For the vast majority of the community, there is absolutely no impact from the licensing change. The SSPL maintains all of the same freedoms the community has always had with MongoDB under AGPL - users are free to use, review, modify, distribute the software or redistribute modifications to the software.

Customers and OEM partners using MongoDB under a commercial license will not be affected by this change.

MongoDB Atlas users do not run the MongoDB database and do not become licensees of the MongoDB database software. As a result, users of MongoDB Atlas will also not be affected by this change.

How can community members contribute to MongoDB repositories under the new license?

Back to Table of Contents

There will be no change for users to contribute to MongoDB repositories under the new license. The process to contribute is documented here.

What will happen if someone in the community is currently building something on MongoDB Community Server?

Back to Table of Contents

There will be no impact to anyone in the community building an application using MongoDB Community Server unless it is a publicly available MongoDB as a service. The copyleft condition of Section 13 of the SSPL does not apply to companies building other applications or a MongoDB as a service offering for internal-only use.

How does this affect customers who use MongoDB as a service from cloud providers today?

Back to Table of Contents

Any publicly available MongoDB as a service offering must comply with the SSPL if they are using a version of MongoDB released on or after October 16, 2018.

Resources

NoSQL Database Explained

MongoDB Architecture Guide

MongoDB Enterprise Advanced

MongoDB Atlas

MongoDB Stitch

MongoDB Engineering Blog

Education & Support

View Course Catalog

Certification

MongoDB Manual

Installation

FAQ

Popular Topics

Migrate to MongoDB Atlas

Building a REST API with MongoDB Stitch

Ingesting and Visualizing API Data with Stitch and Charts

Run MongoDB on AWS with MongoDB Atlas

About

MongoDB, Inc.

Leadership

Email Address

Chapter 8

The Crusade Against Open-source Abuse (Salil Deshpande)

The crusade against open-source abuse

Cloud infrastructure providers threaten the viability of open source

Salil Deshpande@salil / • November 29, 2018

Source: https://techcrunch.com/2018/11/29/the-crusade-against-open-source-abuse/

Image Credits: Brad / Flickr (opens in a new window) under a CC BY 2.0 (opens in a new window) license.

Salil DeshpandeContributor
Salil Deshpande serves as the managing director of Bain Capital Ventures. He focuses on infrastructure software and open source.
More posts by this contributor

- The crusade against open-source abuse

- Commons Clause stops open-source abuse

There's a dark cloud on the horizon. The behavior of cloud infrastructure providers, such as Amazon, threatens the viability of open source. I first wrote about this problem in a prior piece on TechCrunch. In 2018, thankfully, several leaders have mobilized (amid controversy) to propose multiple solutions to the problem. Here's what's happened in the last month.

The Problem

Go to Amazon Web Services (AWS) and hover over the Products menu at the top. You will see numerous open-source projects that Amazon did not create, but run as-a-service. These provide Amazon with billions of dollars of revenue per year. To be clear, this is not illegal. But it is not conducive to sustainable open-source communities, and especially commercial open-source innovation.

Two Solutions

In early 2018, I gathered together the creators, CEOs or general counsels of two dozen at-scale open-source companies, along with respected open-source lawyer Heather Meeker, to talk about what to do.

We wished to define a license that prevents cloud infrastructure providers from running certain software as a commercial service, while at the same time making that software effectively open source for everyone else, i.e. everyone not running that software as a commercial service.

With our first proposal, Commons Clause, we took the most straightforward approach: we constructed one clause, which can be added to any liberal open-source license, preventing the licensee from "Selling" the software — where "Selling" includes running it as a commercial service. (Selling other software made with Commons Clause software is allowed, of course.) Applying Commons Clause transitions a project from open source to source-available.

We also love the proposal being spearheaded by another participant, MongoDB, called the Server Side Public License (SSPL). Rather than prohibit the software from being run as a service, SSPL requires that you open-source all programs that you use to make the software available as a service, including, without limitation, management software, user interfaces, application program interfaces, automation software, monitoring software, backup software, storage software and hosting software, all such that a user could run an instance of the service. This is known as a "copyleft."

These two licenses are two different solutions to exactly the same problem. Heather Meeker wrote both solutions, supported by feedback organized by FOSSA.

The initial uproar and accusations that these efforts were trying to "trick" the community fortunately gave way to understanding and acknowledgement from the open-source community that there is a real problem to be solved here, that it is time for the open-source community to get real and that it is time for the net giants to pay fairly for the open source on which they depend.

In October, one of the board members of the Apache Software Foundation (ASF) reached out to me and suggested working together to create a modern open-source license that solves the industry's needs.

Kudos to MongoDB

Further kudos are owed to MongoDB for definitively stating that they will be using SSPL, submitting SSPL in parallel to an organization called Open Source Initiative (OSI) for endorsement as an open-source license, but not waiting for OSI's endorsement to start releasing software under the SSPL.

OSI, which has somehow anointed itself as the body that will "decide" whether a license is open source, has a habit of myopically debating what's open source and what's not. With the submission of SSPL to OSI, MongoDB has put the ball in OSI's court to either step up and help solve an industry problem, or put their heads back in the sand.

In fact, MongoDB has done OSI a huge favor. MongoDB has gone and solved the problem and handed a perfectly serviceable open-source license to OSI on a silver platter.

Open-source sausage

The public archives of OSI's debate over SSPL are at times informative and at times amusing, bordering on comical. After MongoDB's original submission, there were rah-rah rally cries amongst the members to find reasons to deem SSPL not an open-source license, followed by some +1's. Member John Cowan reminded the group that **just because OSI does not endorse a license as open source, does not mean that it is not open source**:

As far as I know (which is pretty far), the OSI doesn't do that. They have never publicly said "License X is not open source." People on various mailing lists have done so, but not the OSI as such. And they certainly don't say "Any license not on our OSI Certified ™ list is not open source", because that would be false. It's easy to write a license that is obviously open source that the OSI would never certify for any of a variety of reasons.

Eliot Horowitz (CTO and co-founder of MongoDB) responded cogently to questions, comments and objections, concluding with:

In short, we believe that in today's world, linking has been superseded by the provision of programs as services and the connection of programs over networks as the main form of program combination. It is unclear whether existing copyleft licenses clearly apply to this form of program combination, and we intend the SSPL to be an option for developers to address this uncertainty.

Much discussion ensued about the purpose, role and relevance of OSI. Various sundry legal issues were raised or addressed by Van Lindberg, McCoy Smith and Bruce Perens.

Heather Meeker (the lawyer who drafted both Commons Clause and SSPL) stepped in and completely addressed the legal issues that had been raised thus far. Various other clarifications were made by Eliot Horowitz, and he also conveyed willingness to change the wording of the license if it would help.

Discussion amongst the members continued about the role, relevance and purpose of OSI, with one member astutely noting that there were a lot of "free software" wonks in the group, attempting to bastardize open source to advocate their own agenda:

If, instead, OSI has decided that they are now a Free Software organization, and that Free Software is what "we" do, and that "our" focus is on "Free software" then, then let's change the name to the Free Software Initiative and open the gates for some other entity, who is all about Open Source, to take on that job, and do it proudly. :-)

There was debate over whether SSPL discriminates against types of users, which would disqualify it from being open source. Eliot Horowitz provided a convincing explanation that it did not, which seemed to quiet the crowd.

Heather Meeker dropped some more legal knowledge on the group, which seemed to sufficiently address outstanding issues. Bruce Perens, the author of item 6 of the so-called open-source definition, acknowledged that SSPL does not violate item 6 or item 9 of the definition, and subsequently suggested revising item 9 such that SSPL would violate it:

We're not falling on our swords because of this. And we can fix OSD #9 with a two word addition "or performed" as soon as the board can meet. But it's annoying.

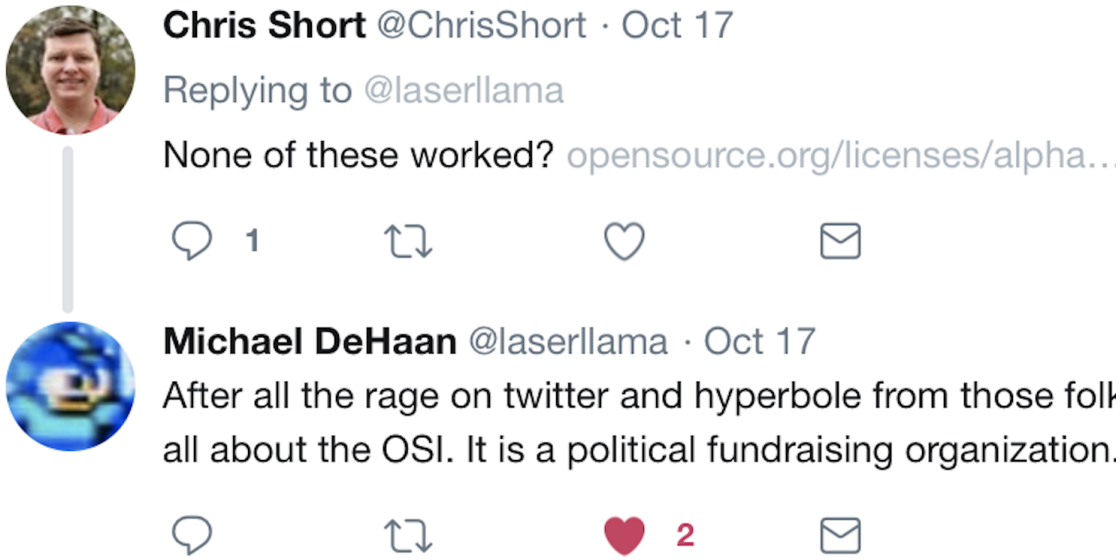
Kyle Mitchell, himself an accomplished open-source lawyer, opposed such a tactic. Larry Rosen pointed out that some members' assertion (that "it is fundamental to open source that everyone can use a program for any purpose") is untrue. Still more entertaining discussion ensued about the purpose of OSI and the meaning of open source.

Carlos Piana succinctly stated why SSPL was indeed open source. Kyle Mitchell added that if licenses were to be judged in the manner that the group was judging SSPL, then GPL v2 was not open source either.

Groundswell

Meanwhile Dor Lior, the founder of database company ScyllaDB, compared SSPL and AGPL side-to-side and argued that "MongoDB would have been better off with Commons Clause or just swallowed a hard pill and stayed with APGL." Player.FM released their service based on Commons Clause-licensed RediSearch, after in-memory database company Redis Labs placed RediSearch and four other specific add-on modules (but not Redis itself) under Commons Clause, and graph database company Neo4J placed its enterprise codebase under Commons Clause and raised an $80 million Series E.

Then Michael DeHaan, creator of Red Hat Ansible, chose Commons Clause for his new project. When asked why he did not choose any of the existing licenses that OSI has "endorsed" to be open source, he said:



This groundswell in 2018 should be ample indication that there is an industry problem that needs to be fixed.

Eliot Horowitz summarized and addressed all the issues, dropped the mic and left for a while. When it seemed like SSPL was indeed following all the rules of open-source licenses, and was garnering support of the members, Brad Kuhn put forward a clumsy argument for why OSI should change the rules as necessary to prevent SSPL from being deemed open source, concluding:

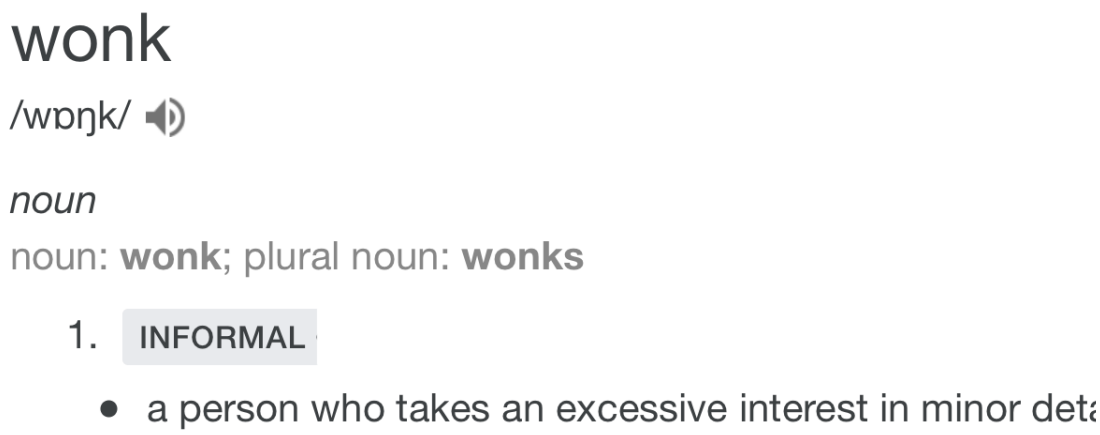
It's likely the entire "license evaluation process" that we use is inherently flawed.

Mitchell clinched the argument that SSPL is open source with definitive points. Horowitz thanked the members for their comments and offered to address any concerns in a revision, and returned a few days later with a revised SSPL.

OSI has 60 days since MongoDB's new submission to make a choice:

1. Wake up and realize that SSPL, perhaps with some edits, is indeed an open-source license, OR
2. Effectively signal to the world that OSI does not wish to help solve the industry's problems, and that they'd rather be policy wonks and have theoretical debates.

"Wonk" here is meant in the best possible way.



Importantly, MongoDB is proceeding to use the SSPL regardless. If MongoDB were going to wait until OSI's decision, or if OSI were more relevant, we might wait with bated breath to hear whether OSI would endorse SSPL as an open-source license.

As it stands, OSI's decision is more important to OSI itself than to the industry. It signals whether OSI wants to remain relevant and help solve industry problems or whether it has become too myopic to be useful. Fearful of the latter, we looked to other groups for leadership and engaged with the Apache Software Foundation (ASF) when they reached out in the hopes of creating a modern open-source license that solves the industry's needs.

OSI should realize that while it would be nice if they deemed SSPL to be open source, it is not critical. Again in the words of John Cowan, just because OSI has not endorsed a license as open source, does not mean it's not open source. While we greatly respect almost all members of industry associations and the work they do in their fields, it is becoming difficult to respect the purpose and process of any group that anoints itself as the body that will "decide" whether a license is open source — it is arbitrary and obsolete.

Errata

In my zest to urge the industry to solve this problem, in an earlier piece, I had said that "if one takes open source software that someone else has built and offers it verbatim as a commercial service for one's own profit" (as cloud infrastructure providers do) that's "not in the spirit" of open source. That's an overstatement and thus, frankly, incorrect. Open source policy wonks pointed this out. I obviously don't mind rattling their cages but I should have stayed away from making statements about "what's in the spirit" so as to not detract from my main argument.

Conclusion

The behavior of cloud infrastructure providers poses an existential threat to open source. Cloud infrastructure providers are not evil. Current open-source licenses allow them to take open-source software verbatim and offer it as a commercial service without giving back to the open-source projects or their commercial shepherds. The problem is that developers do not have open-source licensing alternatives that prevent cloud infrastructure providers from doing so. Open-source standards groups should help, rather than get in the way. We must ensure that authors of open-source software can not only survive, but thrive. And if that means taking a stronger stance against cloud infrastructure providers, then authors should have licenses available to allow for that. The open-source community should make this an urgent priority.

Disclosures

I have not invested directly or indirectly in MongoDB. I have invested directly or indirectly in the companies behind the open source projects Spring, Mule, DynaTrace, Ruby Rails, Groovy Grails, Maven, Gradle, Chef, Redis, SysDig, Prometheus, Hazelcast, Akka, Scala, Cassandra, Spinnaker, FOSSA, and… in Amazon.

Chapter 9

Commons Clause Stops Open-source Abuse (Salil Deshpande)

Commons Clause stops open-source abuse

Salil Deshpande@salil / • September 7, 2018

Source: https://techcrunch.com/2018/09/07/commons-clause-stops-open-source-abuse/

Image Credits: erhui1979 (opens in a new window) / Getty Images

Salil DeshpandeContributor
Salil Deshpande serves as the managing director of Bain Capital Ventures. He focuses on infrastructure software and open source.
More posts by this contributor

- The crusade against open-source abuse
- Commons Clause stops open-source abuse

There's a dark cloud on the horizon. The behavior of cloud infrastructure providers, such as Amazon, threatens the viability of open source.

During 13 years as a venture investor, I have invested in the companies behind many open-source projects:

- Spring
- Mule
- Ruby Rails
- Groovy
- Grails
- Maven
- Gradle
- Redis
- SysDig
- Hazelca
- Akka
- Scala
- Cassandra
- Sp
- and others.

Open source has served society, and open-source business models have been successful and lucrative. Life was good.

Amazon's behavior

I admire Amazon's execution. In the venture business we are used to the large software incumbents (such as IBM, Oracle, HP, Compuware, CA, EMC, VMware, Citrix and others) being primarily big sales and distribution channels, which need to acquire innovation (i.e. startups) to feed their channel. Not Amazon. In July 2015, The Wall Street Journal quoted me as saying, "Amazon executes too well, almost like a startup. This is scary for everyone in the ecosystem." That month, I wrote Fear The Amazon Juggernaut on investor site Seeking Alpha. AMZN is up 400 percent since I wrote that article. (I own AMZN indirectly.)

But to anyone other than its customers, Amazon is not a warm and fuzzy company. Numerous articles have detailed its bruising and cutthroat culture. Why would its use of open source be any different?

Go to Amazon Web Services (AWS) and hover over the Products menu at the top. You will see numerous open-source projects that Amazon did not create, but runs as-a-service. These provide Amazon with billions of dollars of revenue per year.

For example, Amazon takes Redis (the most loved database in StackOverflow's developer survey), gives very little back, and runs it as a service, re-branded as AWS Elasticache. Many other popular open-source projects including, Elasticsearch, Kafka, Postgres, MySQL, Docker, Hadoop, Spark and more, have similarly been taken and offered as AWS products.

To be clear, this is not illegal. But we think it is wrong, and not conducive to sustainable open-source communities.

Commons Clause

In early 2018, I gathered together creators, CEOs or chief counsels of two dozen at-scale open-source companies, some of them public, to talk about what to do. In March I spoke to GeekWire about this effort. After a lot of constructive discussion the group decided that rather than beat around the bush with mixing and matching open-source licenses to discourage such behavior, we should create a straightforward clause that prohibits the behavior. We engaged respected open-source lawyer Heather Meeker to draft this clause.

In August 2018 Redis Labs announced their decision to add this rider (i.e. one additional paragraph) known as the Commons Clause to their liberal open-source license for certain add-on modules. Redis itself would remain on the permissive BSD license — nothing had changed with Redis itself! But the Redis Labs add-on modules will include the Commons Clause rider, which makes the source code available, without the ability to "sell" the modules, where "sell" includes offering them as a commercial service. The goal is to explicitly prevent the bad behavior of cloud infrastructure providers.

Anybody else, including enterprises like General Motors or General Electric, can still do all the things they used to be able to do with the software, even with Commons Clause applied to it. They can view and modify the source code and submit pull-requests to get their modifications into the product. They can even offer the software as-a-service internally for employees. What Commons Clause prevents is the running of a commercial service with somebody else's open-source software in the manner that cloud infrastructure providers do.

This announcement has — unsurprisingly, knowing the open-source community — prompted spirited responses, both favorable and critical. At the risk of oversimplifying: those in favo view this as a logical and positive evolutio in open-source licensing that allows open-source companies to run viable businesses while investing in open-source projects. Michael DeHaan, creator of Ansible, in Why Open Source Needs New Licenses, put one part particularly well:

> We see people running open source "foundations" and web sites that are essentially talking heads, spewing political arguments about the definition of "open source" as described by something called "The Open Source Initiative", which contains various names which have attained some level of popularity or following. They attempt to state that such a license where the source code is freely available, but use cases are limited, are "not open source". Unfortunately, that ship has sailed.

Those neutral or against

First, do not worry about Redis Labs. The company is doing very, very well. And Redis is stronger, more loved and more BSD than ever before.

More importantly, we think it is time to reexamine the ethos of open source in today's environment. When open source became popular, it was designed for practitioners to experiment with and build on, while contributing back to the community. No company was providing infrastructure as a service. No company was taking an open-source project, re-branding it, running it as a service, keeping the profits and giving very little back.

Our view is that open-source software was never intended for cloud infrastructure companies to take and sell. That is not the original ethos of open source. Commons Clause is reviving the original ethos of open source. Academics, hobbyists or developers wishing to use a popular open-source project to power a component of their application can still do so. But if you want to take substantially the same software that someone else has built, and offer it as a service, for your own profit, that's not in the spirit of the open-source community.

As it turns out in the case of the Commons Clause, that can make the source code not technically open source. But that is something we must live with, to preserve the original ethos.

Apache + Commons Clause

Redis Labs released certain add-on modules as Apache + Commons Clause. Redis Labs made amply clear that the application of Commons Clause made them not open source, and that Redis itself remains open source and BSD-licensed.

Some rabid open-source wonks accused Redis Labs of trying to trick the community into thinking that modules were open source, because they used the word "Apache." (They were reported to be foaming at the mouth while making these accusations, but in fairness it could have been just drool.)

There's no trick. The Commons Clause is a rider that is to be attached to any permissive open-source license. Because various open-source projects use various open-source licenses, when releasing software using Commons Clause, one must specify to which underlying permissive open-source license one is attaching Commons Clause.

Why not AGPL?

There are two key reasons to not use AGPL in this scenario, an open-source license that says that you must release to the public any modifications you make when you run AGPL-licensed code as a service.

First, AGPL makes it inconvenient but does not prevent cloud infrastructure providers from engaging in the abusive behavior described above. It simply says that they must release any modifications they make while engaging in such behavior. Second, AGPL contains language about software patents that is unnecessary and disliked by a number of enterprises.

Many of our portfolio companies with AGPL projects have received requests from large enterprises to move to a more permissive license, since the use of AGPL is against their company's policy.

Balance

Cloud infrastructure providers are not bad guys or acting with bad intentions. Open source has always been a balancing act. Many of us believe in our customers and peers seeing our source code, making improvements and sharing back. It's always a leap of faith to distribute one's work product for free and to trust that you'll be able to put food on the table. Sometimes, with some projects, a natural balance occurs without much deliberate effort. But at other times, the natural balance does not occur: We are seeing this more and more with infrastructure open source, especially as cloud infrastructure providers seek to differentiate by moving up the stack from commodity compute and storage to higher level infrastructure services.

Revisions

The Commons Clause as of this writing is at version 1.0. There will be revisions and tweaks in the future to ensure that Commons Clause implements its goals. We'd love your input.

Differences of opinion on Commons Clause that we have seen expressed so far are essentially differences of philosophy. Much criticism has come from open-source wonks who are not in the business of making money with software. They have a different philosophy, but that is not surprising, because their job is to be political activists, not build value in companies.

Some have misconstrued that it prevents people from offering maintenance, support or professional services. This is a misreading of the language. Some have claimed that it conflicts with AGPL. Commons Clause is intended to be used with open-source licenses that are more permissive than AGPL, so that AGPL does not have to be used! Still, even with AGPL, few users of an author's work would deem it prudent to simply disregard an author's statement of intent to apply Commons Clause.

Protecting open source

Some open-source stakeholders are confused. Whose side should they be on? Commons Clause is new, and we expected debate. The people behind this initiative are committed open-source advocates, and our intent is to protect open source from an existential threat. We hope others will rally to the cause, so that open-source companies can make money, open source can be viable and open-source developers can get paid for their contributions.

Chapter 10

Anarchism Triumphant: Free Software and the Death of Copyright (Eben Moglen)

Anarchism Triumphant: Free Software and the Death of Copyright

Eben Moglen*

May 17, 1999

I Software as Property: The Theoretical Paradox

SOFTWARE: no other word so thoroughly connotes the practical and social effects of the digital revolution. Originally, the term was purely technical, and denoted the parts of a computer system that, unlike "hardware," which was unchangeably manufactured in system electronics, could be altered freely. The first software amounted to the plug configuration of cables or switches on the outside panels of an electronic device, but as soon as linguistic means of altering computer behavior had been developed, "software" mostly denoted the expressions in more or less human-readable language that both described and controlled machine behavior.[1]

* Professor of Law & Legal History, Columbia Law School. Prepared for delivery at the Buchmann International Conference on Law, Technology and Information, at Tel Aviv University, May 1999; my thanks to the organizers for their kind invitation. I owe much as always to Pamela Karlan for her insight and encouragement. Thanks are due to Jerome Saltzer, Richard Stallman, and numerous others who freely contributed corrections and impovements to this paper. I especially wish to thank the programmers throughout the world who made free software possible.

[1] The distinction was only approximate in its original context. By the late 1960s certain portions of the basic operation of hardware were controlled by programs digitally encoded in the electronics of computer equipment, not subject to change after the units left the factory. Such symbolic but unmodifiable components were known in the trade as "microcode," but it became conventional to refer to them as "firmware." Softness, the term "firmware" demonstrated, referred primarily to users' ability to alter symbols determining machine behavior. As the digital revolution has resulted in the widespread use of computers by technical incompetents, most traditional software—application programs, operating

That was then and this is now. Technology based on the manipulation of digitally-encoded information is now socially dominant in most aspects of human culture in the "developed" societies.[2] The movement from analog to digital representation—in video, music, printing, telecommunications, and even choreography, religious worship, and sexual gratification—potentially turns all forms of human symbolic activity into software, that is, modifiable instructions for describing and controlling the behavior of machines. By a conceptual back-formation characteristic of Western scientistic thinking, the division between hardware and software is now being observed in the natural or social world, and has become a new way to express the conflict between ideas of determinism and free will, nature and nurture, or genes and culture. Our "hardware," genetically wired, is our nature, and determines us. Our nurture is "software," establishes our cultural programming, which is our comparative freedom. And so on, for those reckless of blather.[3] Thus "software" becomes a viable metaphor for all symbolic activity, apparently divorced from the technical context of the word's origin, despite the unease raised in the technically competent when the term is thus bandied about, eliding the conceptual significance of its derivation.[4]

But the widespread adoption of digital technology for use by those who do not understand the principles of its operation, while it apparently licenses the broad metaphoric employment of "software," does not in fact permit us to ignore the computers that are now everywhere underneath our social skin. The movement from analog to digital is more important for the structure of social and legal relations than the more famous if less

systems, numerical control instructions, and so forth—is, for most of its users, firmware. It may be symbolic rather than electronic in its construction, but they couldn't change it even if they wanted to, which they often—impotently and resentfully—do. This "firming of software" is a primary condition of the propertarian approach to the legal organization of digital society, which is the subject of this paper.

[2]Within the present generation, the very conception of social "development" is shifting away from possession of heavy industry based on the internal-combustion engine to "post-industry" based on digital communications and the related "knowledge-based" forms of economic activity.

[3]Actually, a moment's thought will reveal, our genes are firmware. Evolution made the transition from analog to digital before the fossil record begins. But we haven't possessed the power of controlled direct modification. Until the day before yesterday. In the next century the genes too will become software, and while I don't discuss the issue further in this paper, the political consequences of unfreedom of software in this context are even more disturbing than they are with respect to cultural artifacts.

[4]*See, e.g.*, J. M. Balkin, *Cultural Software: a Theory of Ideology* (New Haven: Yale University Press, 1998).

certain movement from status to contract.[5] This is bad news for those legal thinkers who do not understand it, which is why so much pretending to understand now goes so floridly on. Potentially, however, our great transition is very good news for those who can turn this new-found land into property for themselves. Which is why the current "owners" of software so strongly support and encourage the ignorance of everyone else. Unfortunately for them—for reasons familiar to legal theorists who haven't yet understood how to apply their traditional logic in this area—the trick won't work. This paper explains why.[6]

We need to begin by considering the technical essence of the familiar devices that surround us in the era of "cultural software." A CD player is a good example. Its primary input is a bitstream read from an optical storage disk. The bitstream describes music in terms of measurements, taken 44,000 times per second, of frequency and amplitude in each of two audio channels. The player's primary output is analog audio signals.[7] Like everything else in the digital world, music as seen by a CD player is mere numeric information; a particular recording of Beethoven's Ninth Symphony recorded by Arturo Toscanini and the NBC Symphony Orchestra and Chorale is (to drop a few insignificant digits) 1276749873424, while Glenn Gould's peculiarly perverse last recording of the Goldberg Variations is (similarly rather truncated) 767459083268.

[5] *See* Henry Sumner Maine, *Ancient Law: Its Connection with the Early History of Society, and its Relation to Modern Ideas*, 1st edn. (London: J. Murray, 1861).

[6] In general I dislike the intrusion of autobiography into scholarship. But because it is here my sad duty and great pleasure to challenge the qualifications or *bona fides* of just about everyone, I must enable the assessment of my own. I was first exposed to the craft of computer programming in 1971. I began earning wages as a commercial programmer in 1973—at the age of thirteen—and did so, in a variety of computer services, engineering, and multinational technology enterprises, until 1985. In 1975 I helped write one of the first networked email systems in the United States; from 1979 I was engaged in research and development of advanced computer programming languages at IBM. These activities made it economically possible for me to study the arts of historical scholarship and legal cunning. My wages were sufficient to pay my tuitions, but not—to anticipate an argument that will be made by the econodwarves further along—because my programs were the intellectual property of my employer, but rather because they made the hardware my employer sold work better. Most of what I wrote was effectively free software, as we shall see. Although I subsequently made some inconsiderable technical contributions to the actual free software movement this paper describes, my primary activities on its behalf have been legal: I have served for the past five years (without pay, naturally) as general counsel of the Free Software Foundation.

[7] The player, of course, has secondary inputs and outputs in control channels: buttons or infrared remote control are input, and time and track display are output.

Oddly enough, these two numbers are "copyrighted." This means, supposedly, that you can't possess another copy of these numbers, once fixed in any physical form, unless you have licensed them. And you can't turn 767459083268 into 2347895697 for your friends (thus correcting Gould's ridiculous judgment about tempi) without making a "derivative work," for which a license is necessary.

At the same time, a similar optical storage disk contains another number, let us call it 7537489532. This one is an algorithm for linear programming of large systems with multiple constraints, useful for example if you want to make optimal use of your rolling stock in running a freight railroad. This number (in the US) is "patented," which means you cannot derive 7537489532 for yourself, or otherwise "practice the art" of the patent with respect to solving linear programming problems no matter how you came by the idea, including finding it out for yourself, unless you have a license from the number's owner.

Then there's 9892454959483. This one is the source code for Microsoft Word. In addition to being "copyrighted," this one is a trade secret. That means if you take this number from Microsoft and give it to anyone else you can be punished.

Lastly, there's 588832161316. It doesn't do anything, it's just the square of 767354. As far as I know, it isn't owned by anybody under any of these rubrics. Yet.

At this point we must deal with our first objection from the learned. It comes from a creature known as the IPdroid. The droid has a sophisticated mind and a cultured life. It appreciates very much the elegant dinners at academic and ministerial conferences about the TRIPs, not to mention the privilege of frequent appearances on MSNBC. It wants you to know that I'm committing the mistake of confusing the embodiment with the intellectual property itself. It's not the number that's patented, stupid, just the Kamarkar algorithm. The number *can* be copyrighted, because copyright covers the expressive qualities of a particular tangible embodiment of an idea (in which some functional properties may be mysteriously merged, provided that they're not too merged), but not the algorithm. Whereas the number isn't patentable, just the "teaching" of the number with respect to making railroads run on time. And the number representing the source code of Microsoft Word can be a trade secret, but if you find it out for yourself (by performing arithmetic manipulation of other numbers issued by Microsoft, for example, which is known as "reverse engineering"), you're not going to be punished, at least if you live in some parts of the United States.

This droid, like other droids, is often right. The condition of being a droid is to know everything about something and nothing about anything else. By its timely and urgent intervention the droid has established that the current intellectual property system contains many intricate and ingenious features. The complexities combine to allow professors to be erudite, Congressmen to get campaign contributions, lawyers to wear nice suits and tassel loafers, and Murdoch to be rich. The complexities mostly evolved in an age of industrial information distribution, when information was inscribed in analog forms on physical objects that cost something significant to make, move, and sell. When applied to digital information that moves frictionlessly through the network and has zero marginal cost per copy, everything still works, mostly, as long as you don't stop squinting.

But that wasn't what I was arguing about. I wanted to point out something else: that our world consists increasingly of nothing but large numbers (also known as bitstreams), and that—for reasons having nothing to do with emergent properties of the numbers themselves—the legal system is presently committed to treating similar numbers radically differently. No one can tell, simply by looking at a number that is 100 million digits long, whether that number is subject to patent, copyright, or trade secret protection, or indeed whether it is "owned" by anyone at all. So the legal system we have—blessed as we are by its consequences if we are copyrights teachers, Congressmen, Gucci-gulchers or Big Rupert himself—is compelled to treat indistinguishable things in unlike ways.

Now, in my role as a legal historian concerned with the secular (that is, very long term) development of legal thought, I claim that legal regimes based on sharp but unpredictable distinctions among similar objects are radically unstable. They fall apart over time because every instance of the rules' application is an invitation to at least one side to claim that instead of fitting in ideal category A the particular object in dispute should be deemed to fit instead in category B, where the rules will be more favorable to the party making the claim. This game—about whether a typewriter should be deemed a musical instrument for purposes of railway rate regulation, or whether a steam shovel is a motor vehicle—is the frequent stuff of legal ingenuity. But when the conventionally-approved legal categories require judges to distinguish among the identical, the game is infinitely lengthy, infinitely costly, and almost infinitely offensive to the unbiased bystander.[8]

[8]This is not an insight unique to our present enterprise. A closely-related idea forms one of the most important principles in the history of Anglo-American law, perfectly put by Toby Milsom in the following terms:

Thus parties can spend all the money they want on all the legislators and judges they can afford—which for the new "owners" of the digital world is quite a few—but the rules they buy aren't going to work in the end. Sooner or later, the paradigms are going to collapse. Of course, if later means two generations from now, the distribution of wealth and power sanctified in the meantime may not be reversible by any course less drastic than a *bellum servile* of couch potatoes against media magnates. So knowing that history isn't on Bill Gates' side isn't enough. We are predicting the future in a very limited sense: we know that the existing rules, which have yet the fervor of conventional belief solidly enlisted behind them, are no longer meaningful. Parties will use and abuse them freely until the mainstream of "respectable" conservative opinion acknowledges their death, with uncertain results. But realistic scholarship should already be turning its attention to the clear need for new thoughtways.

* * * * *

When we reach this point in the argument, we find ourselves contending with the other primary protagonist of educated idiocy: the econodwarf. Like the IPdroid, the econodwarf is a species of hedgehog,[9] but where the droid is committed to logic over experience, the econodwarf specializes in an energetic and well-focused but entirely erroneous view of human nature. According to the econodwarf's vision, each human being is an individual possessing "incentives," which can be retrospectively unearthed by imagining the state of the bank account at various times. So in this instance the econodwarf feels compelled to object that without the rules I am lampooning, there would be no incentive to create the things the rules treat as property: without the ability to exclude others from music there would be no music, because no one could be sure of getting paid for creating it.

> The life of the common law has been in the abuse of its elementary ideas. If the rules of property give what now seems an unjust answer, try obligation; and equity has proved that from the materials of obligation you can counterfeit the phenomena of property. If the rules of contract give what now seems an unjust answer, try tort. ... If the rules of one tort, say deceit, give what now seems an unjust answer, try another, try negligence. And so the legal world goes round.
>
> S. F. C. Milsom, *Historical Foundations of the Common Law*, 2nd edn. (London: Butterworths, 1981), 6.

[9] *See* Isaiah Berlin, *The Hedgehog and the Fox; an Essay on Tolstoy's View of History* (New York: Simon and Schuster, 1953).

Music is not really our subject; the software I am considering at the moment is the old kind: computer programs. But as he is determined to deal at least cursorily with the subject, and because, as we have seen, it is no longer really possible to distinguish computer programs from music performances, a word or two should be said. At least we can have the satisfaction of indulging in an argument *ad pygmeam*. When the econodwarf grows rich, in my experience, he attends the opera. But no matter how often he hears *Don Giovanni* it never occurs to him that Mozart's fate should, on his logic, have entirely discouraged Beethoven, or that we have *The Magic Flute* even though Mozart knew very well he wouldn't be paid. In fact, *The Magic Flute*, the *St. Matthew's Passion*, and the motets of the wife-murderer Carlo Gesualdo are all part of the centuries-long tradition of free software, in the more general sense, which the econodwarf never quite acknowledges.

The dwarf's basic problem is that "incentives" is merely a metaphor, and as a metaphor to describe human creative activity it's pretty crummy. I have said this before,[10] but the better metaphor arose on the day Michael Faraday first noticed what happened when he wrapped a coil of wire around a magnet and spun the magnet. Current flows in such a wire, but we don't ask what the incentive is for the electrons to leave home. We say that the current results from an emergent property of the system, which we call induction. The question we ask is "what's the resistance of the wire?" So Moglen's Metaphorical Corollary to Faraday's Law says that if you wrap the Internet around every person on the planet and spin the planet, software flows in the network. It's an emergent property of connected human minds that they create things for one another's pleasure and to conquer their uneasy sense of being too alone. The only question to ask is, what's the resistance of the network? Moglen's Metaphorical Corollary to Ohm's Law states that the resistance of the network is directly proportional to the field strength of the "intellectual property" system. So the right answer to the econodwarf is, resist the resistance.

Of course, this is all very well in theory. "Resist the resistance" sounds good, but we'd have a serious problem, theory notwithstanding, if the dwarf were right and we found ourselves under-producing good software because we didn't let people own it. But dwarves and droids are formalists of different kinds, and the advantage of realism is that if you start from the facts the facts are always on your side. It turns out that treating software as property makes bad software.

[10] See The Virtual Scholar and Network Liberation.
http://emoglen.law.columbia.edu/my_pubs/nospeech.html

II Software as Property: The Practical Problem

In order to understand why turning software into property produces bad software, we need an introduction to the history of the art. In fact, we'd better start with the word "art" itself. The programming of computers combines determinate reasoning with literary invention.

At first glance, to be sure, source code appears to be a non-literary form of composition.[11] The primary desideratum in a computer program is that it works, that is to say, performs according to specifications formally describing its outputs in terms of its inputs. At this level of generality, the functional content of programs is all that can be seen.

But working computer programs exist as parts of computer systems, which are interacting collections of hardware, software, and human beings. The human components of a computer system include not only the users, but also the (potentially different) persons who maintain and improve the system. Source code not only communicates with the computer that executes the program, through the intermediary of the compiler that produces machine-language object code, but also with other programmers.

The function of source code in relation to other human beings is not widely grasped by non-programmers, who tend to think of computer programs as incomprehensible. They would be surprised to learn that the bulk of information contained in most programs is, from the point of view of the compiler or other language processor, "comment," that is, non-functional material. The comments, of course, are addressed to others who may need to fix a problem or to alter or enhance the program's operation. In most programming languages, far more space is spent in telling people what the program does than in telling the computer how to do it.

The design of programming languages has always proceeded under the dual requirements of complete specification for machine execution and informative description for human readers. One might identify three basic

[11] Some basic vocabulary is essential. Digital computers actually execute numerical instructions: bitstrings that contain information in the "native" language created by the machine's designers. This is usually referred to as "machine language." The machine languages of hardware are designed for speed of execution at the hardware level, and are not suitable for direct use by human beings. So among the central components of a computer system are "programming languages," which translate expressions convenient for humans into machine language. The most common and relevant, but by no means the only, form of computer language is a "compiler." The compiler performs static translation, so that a file containing human-readable instructions, known as "source code" results in the generation of one or more files of executable machine language, known as "object code."

strategies in language design for approaching this dual purpose. The first, pursued initially with respect to the design of languages specific to particular hardware products and collectively known as "assemblers," essentially separated the human- and machine-communication portions of the program. Assembler instructions are very close relatives of machine-language instructions: in general, one line of an assembler program corresponds to one instruction in the native language of the machine. The programmer controls machine operation at the most specific possible level, and (if well-disciplined) engages in running commentary alongside the machine instructions, pausing every few hundred instructions to create "block comments," which provide a summary of the strategy of the program, or document the major data structures the program manipulates.

A second approach, characteristically depicted by the language COBOL (which stood for "Common Business-Oriented Language"), was to make the program itself look like a set of natural language directions, written in a crabbed but theoretically human-readable style. A line of COBOL code might say, for example "MULTIPLY PRICE TIMES QUANTITY GIVING EXPANSION." At first, when the Pentagon and industry experts began the joint design of COBOL in the early 1960s, this seemed a promising approach. COBOL programs appeared largely self-documenting, allowing both the development of work teams able to collaborate on the creation of large programs, and the training of programmers who, while specialized workers, would not need to understand the machine as intimately as assembler programs had to. But the level of generality at which such programs documented themselves was wrongly selected. A more formulaic and compressed expression of operational detail "expansion = price x quantity," for example, was better suited even to business and financial applications where the readers and writers of programs were accustomed to mathematical expression, while the processes of describing both data structures and the larger operational context of the program were not rendered unnecessary by the wordiness of the language in which the details of execution were specified.

Accordingly, language designers by the late 1960s began experimenting with forms of expression in which the blending of operational details and non-functional information necessary for modification or repair was more subtle. Some designers chose the path of highly symbolic and compressed languages, in which the programmer manipulated data abstractly, so that "A x B" might mean the multiplication of two integers, two complex numbers, two vast arrays, or any other data type capable of some process called

"multiplication," to be undertaken by the computer on the basis of the context for the variables "A" and "B" at the moment of execution.[12] Because this approach resulted in extremely concise programs, it was thought, the problem of making code comprehensible to those who would later seek to modify or repair it was simplified. By hiding the technical detail of computer operation and emphasizing the algorithm, languages could be devised that were better than English or other natural languages for the expression of stepwise processes. Commentary would be not only unnecessary but distracting, just as the metaphors used to convey mathematical concepts in English do more to confuse than to enlighten.

A How We Created the Microbrain Mess

Thus the history of programming languages directly reflected the need to find forms of human-machine communication that were also effective in conveying complex ideas to human readers. "Expressivity" became a property of programming languages, not because it facilitated computation, but because it facilitated the collaborative creation and maintenance of increasingly complex software systems.

At first impression, this seems to justify the application of traditional copyright thinking to the resulting works. Though substantially involving "functional" elements, computer programs contained "expressive" features of paramount importance. Copyright doctrine recognized the merger of function and expression as characteristic of many kinds of copyrighted works. "Source code," containing both the machine instructions necessary for functional operation and the expressive "commentary" intended for human readers, was an appropriate candidate for copyright treatment.

True, so long as it is understood that the expressive component of software was present solely in order to facilitate the making of "derivative works." Were it not for the intention to facilitate alteration, the expressive elements of programs would be entirely supererogatory, and source code would be no more copyrightable than object code, the output of the language processor, purged of all but the program's functional characteristics.

The state of the computer industry throughout the 1960s and 1970s, when the grundnorms of sophisticated computer programming were established,

[12] This, I should say, was the path that most of my research and development followed, largely in connection with a language called APL ("A Programming Language") and its successors. It was not, however, the ultimately-dominant approach, for reasons that will be suggested below.

concealed the tension implicit in this situation. In that period, hardware was expensive. Computers were increasingly large and complex collections of machines, and the business of designing and building such an array of machines for general use was dominated, not to say monopolized, by one firm. IBM gave away its software. To be sure, it owned the programs its employees wrote, and it copyrighted the source code. But it also distributed the programs—including the source code—to its customers at no additional charge, and encouraged them to make and share improvements or adaptations of the programs thus distributed. For a dominant hardware manufacturer, this strategy made sense: better programs sold more computers, which is where the profitability of the business rested.

Computers, in this period, tended to aggregate within particular organizations, but not to communicate broadly with one another. The software needed to operate was distributed not through a network, but on spools of magnetic tape. This distribution system tended to centralize software development, so that while IBM customers were free to make modifications and improvements to programs, those modifications were shared in the first instance with IBM, which then considered whether and in what way to incorporate those changes in the centrally-developed and distributed version of the software. Thus in two important senses the best computer software in the world was free: it cost nothing to acquire, and the terms on which it was furnished both allowed and encouraged experimentation, change, and improvement.[13] That the software in question was IBM's property under prevailing copyright law certainly established some theoretical limits on users' ability to distribute their improvements or adaptations to others, but in practice mainframe software was cooperatively developed by the dominant hardware manufacturer and its technically-sophisticated users, employing the manufacturer's distribution resources to propagate the resulting improvements through the user community. The right to exclude others, one of the most important "sticks in the bundle" of property

[13]This description elides some details. By the mid-1970s IBM had acquired meaningful competition in the mainframe computer business, while the large-scale antitrust action brought against it by the US government prompted the decision to "unbundle," or charge separately, for software. In this less important sense, software ceased to be free. But—without entering into the now-dead but once-heated controversy over IBM's software pricing policies—the unbundling revolution had less effect on the social practices of software manufacture than might be supposed. As a fellow responsible for technical improvement of one programming language product at IBM from 1979 to 1984, for example, I was able to treat the product as "almost free," that is, to discuss with users the changes they had proposed or made in the programs, and to engage with them in cooperative development of the product for the benefit of all users.

rights (in an image beloved of the United States Supreme Court), was practically unimportant, or even undesirable, at the heart of the software business.[14]

After 1980, everything was different. The world of mainframe hardware gave way within ten years to the world of the commodity PC. And, as a contingency of the industry's development, the single most important element of the software running on that commodity PC, the operating system, became the sole significant product of a company that made no hardware. High-quality basic software ceased to be part of the product-differentiation strategy of hardware manufacturers. Instead, a firm with an overwhelming share of the market, and with the near-monopolist's ordinary absence of interest in fostering diversity, set the practices of the software industry. In such a context, the right to exclude others from participation in the product's formation became profoundly important. Microsoft's power in the market rested entirely on its ownership of the Windows source code.

To Microsoft, others' making of "derivative works," otherwise known as repairs and improvements, threatened the central asset of the business. Indeed, as subsequent judicial proceedings have tended to establish, Microsoft's strategy as a business was to find innovative ideas elsewhere in the software marketplace, buy them up and either suppress them or incorporate them in its proprietary product. The maintenance of control over the basic operation of computers manufactured, sold, possessed, and used by others represented profound and profitable leverage over the development of the culture;[15] the right to exclude returned to center stage in the concept of software as property.

The result, so far as the quality of software was concerned, was disastrous. The monopoly was a wealthy and powerful corporation that employed a large number of programmers, but it could not possibly afford the number of testers, designers, and developers required to produce flex-

[14]This description is highly compressed, and will seem both overly simplified and unduly rosy to those who also worked in the industry during this period of its development. Copyright protection of computer software was a controversial subject in the 1970s, leading to the famous CONTU commission and its mildly pro-copyright recommendations of 1979. And IBM seemed far less cooperative to its users at the time than this sketch makes out. But the most important element is the contrast with the world created by the PC, the Internet, and the dominance of Microsoft, with the resulting impetus for the free software movement, and I am here concentrating on the features that express that contrast.

[15]I discuss the importance of PC software in this context, the evolution of "the market for eyeballs" and "the sponsored life" in other chapters of my forthcoming book, *The Invisible Barbecue*, of which this essay forms a part.

ible, robust and technically-innovative software appropriate to the vast array of conditions under which increasingly ubiquitous personal computers operated. Its fundamental marketing strategy involved designing its product for the least technically-sophisticated users, and using "fear, uncertainty, and doubt" (known within Microsoft as "FUD") to drive sophisticated users away from potential competitors, whose long-term survivability in the face of Microsoft's market power was always in question.

Without the constant interaction between users able to repair and improve and the operating system's manufacturer, the inevitable deterioration of quality could not be arrested. But because the personal computer revolution expanded the number of users exponentially, almost everyone who came in contact with the resulting systems had nothing against which to compare them. Unaware of the standards of stability, reliability, maintainability and effectiveness that had previously been established in the mainframe world, users of personal computers could hardly be expected to understand how badly, in relative terms, the monopoly's software functioned. As the power and capacity of personal computers expanded rapidly, the defects of the software were rendered less obvious amidst the general increase of productivity. Ordinary users, more than half afraid of the technology they almost completely did not understand, actually welcomed the defectiveness of the software. In an economy undergoing mysterious transformations, with the concomitant destabilization of millions of careers, it was tranquilizing, in a perverse way, that no personal computer seemed to be able to run for more than a few consecutive hours without crashing. Although it was frustrating to lose work in progress each time an unnecessary failure occurred, the evident fallibility of computers was intrinsically reassuring.[16]

None of this was necessary. The low quality of personal computer software could have been reversed by including users directly in the inherently evolutionary process of software design and implementation. A Lamarckian mode, in which improvements could be made anywhere, by anyone, and inherited by everyone else, would have wiped out the deficit, restoring to the world of the PC the stability and reliability of the software made in the quasi-propertarian environment of the mainframe era. But the Microsoft business model precluded Lamarckian inheritance of software improvements. Copyright doctrine, in general and as it applies to software in

[16]This same pattern of ambivalence, in which bad programming leading to widespread instability in the new technology is simultaneously frightening and reassuring to technical incompetents, can be seen also in the primarily-American phenomenon of Y2K hysteria.

particular, biases the world towards creationism; in this instance, the problem is that BillG the Creator was far from infallible, and in fact he wasn't even trying.

To make the irony more severe, the growth of the network rendered the non-propertarian alternative even more practical. What scholarly and popular writing alike denominate as a thing ("the Internet") is actually the name of a social condition: the fact that everyone in the network society is connected directly, without intermediation, to everyone else.[17] The global interconnection of networks eliminated the bottleneck that had required a centralized software manufacturer to rationalize and distribute the outcome of individual innovation in the era of the mainframe.

And so, in one of history's little ironies, the global triumph of bad software in the age of the PC was reversed by a surprising combination of forces: the social transformation initiated by the network, a long-discarded European theory of political economy, and a small band of programmers throughout the world mobilized by a single simple idea.

B Software Wants to Be Free; or, How We Stopped Worrying and Learned to Love the Bomb

Long before the network of networks was a practical reality, even before it was an aspiration, there was a desire for computers to operate on the basis of software freely available to everyone. This began as a reaction against propertarian software in the mainframe era, and requires another brief historical digression.

Even though IBM was the largest seller of general purpose computers in the mainframe era, it was not the largest designer and builder of such hardware. The telephone monopoly, American Telephone & Telegraph, was in fact larger than IBM, but it consumed its products internally. And at the famous Bell Labs research arm of the telephone monopoly, in the late 1960s, the developments in computer languages previously described gave birth to an operating system called Unix.

The idea of Unix was to create a single, scalable operating system to exist on all the computers, from small to large, that the telephone monopoly made for itself. To achieve this goal meant writing an operating system not in machine language, nor in an assembler whose linguistic form was

[17] The critical implications of this simple observation about our metaphors are worked out in "How Not to Think about 'The Internet'," in *The Invisible Barbecue*, forthcoming.

integral to a particular hardware design, but in a more expressive and generalized language. The one chosen was also a Bell Labs invention, called "C."[18] The C language became common, even dominant, for many kinds of programming tasks, and by the late 1970s the Unix operating system written in that language had been transferred (or "ported," in professional jargon) to computers made by many manufacturers and of many designs.

AT&T distributed Unix widely, and because of the very design of the operating system, it had to make that distribution in C source code. But AT&T retained ownership of the source code and compelled users to purchase licenses that prohibited redistribution and the making of derivative works. Large computing centers, whether industrial or academic, could afford to purchase such licenses, but individuals could not, while the license restrictions prevented the community of programmers who used Unix from improving it in an evolutionary rather than episodic fashion. And as programmers throughout the world began to aspire to and even expect a personal computer revolution, the "unfree" status of Unix became a source of concern.

Between 1981 and 1984, one man envisioned a crusade to change the situation. Richard M. Stallman, then an employee of MIT's Artificial Intelligence Laboratory, conceived the project of independent, collaborative redesign and implementation of an operating system that would be true free software. In Stallman's phrase, free software would be a matter of freedom, not of price. Anyone could freely modify and redistribute such software, or sell it, subject only to the restriction that he not try to reduce the rights of others to whom he passed it along. In this way free software could become a self-organizing project, in which no innovation would be lost through proprietary exercises of rights. The system, Stallman decided, would be called GNU, which stood (in an initial example of a taste for recursive acronyms that has characterized free software ever since), for "GNU's Not Unix." Despite misgivings about the fundamental design of Unix, as well as its terms of distribution, GNU was intended to benefit from the wide if unfree source distribution of Unix. Stallman began Project GNU by writing components of the eventual system that were also designed to work without modification on existing Unix systems. Development of the GNU tools could thus proceed directly in the environment of university and other advanced computing centers around the world.

[18]Technical readers will again observe that this compresses developments occurring from 1969 through 1973.

The scale of such a project was immense. Somehow, volunteer programmers had to be found, organized, and set to work building all the tools that would be necessary for the ultimate construction. Stallman himself was the primary author of several fundamental tools. Others were contributed by small or large teams of programmers elsewhere, and assigned to Stallman's project or distributed directly. A few locations around the developing network became archives for the source code of these GNU components, and throughout the 1980s the GNU tools gained recognition and acceptance by Unix users throughout the world. The stability, reliability, and maintainability of the GNU tools became a by-word, while Stallman's profound abilities as a designer continued to outpace, and provide goals for, the evolving process. The award to Stallman of a MacArthur Fellowship in 1990 was an appropriate recognition of his conceptual and technical innovations and their social consequences.

Project GNU, and the Free Software Foundation to which it gave birth in 1985, were not the only source of free software ideas. Several forms of copyright license designed to foster free or partially free software began to develop in the academic community, mostly around the Unix environment. The University of California Berkeley began the design and implementation of another version of Unix for free distribution in the academic community. BSD Unix, as it came to be known, also treated AT&T's Unix as a design standard. The code was broadly released and constituted a reservoir of tools and techniques, but its license terms limited the range of its application, while the elimination of hardware-specific proprietary code from the distribution meant that no one could actually build a working operating system for any particular computer from BSD. Other university-based work also eventuated in quasi-free software; the graphical user interface (or GUI) for Unix systems called X Windows, for example, was created at MIT and distributed with source code on terms permitting free modification. And in 1989-1990, an undergraduate computer science student at the University of Helsinki, Linus Torvalds, began the project that completed the circuit and fully energized the free software vision.

What Torvalds did was to begin adapting a computer science teaching tool for real life use. Andrew Tannenbaum's MINIX kernel,[19] was a staple

[19]Operating systems, even Windows (which hides the fact from its users as thoroughly as possible), are actually collections of components, rather than undivided unities. Most of what an operating system does (manage file systems, control process execution, etc.) can be abstracted from the actual details of the computer hardware on which the operating system runs. Only a small inner core of the system must actually deal with the eccentric peculiar-

of Operating Systems courses, providing an example of basic solutions to basic problems. Slowly, and at first without recognizing the intention, Linus began turning the MINIX kernel into an actual kernel for Unix on the Intel x86 processors, the engines that run the world's commodity PCs. As Linus began developing this kernel, which he named Linux, he realized that the best way to make his project work would be to adjust his design decisions so that the existing GNU components would be compatible with his kernel.

The result of Torvalds' work was the release on the net in 1991 of a sketchy working model of a free software kernel for a Unix-like operating system for PCs, fully compatible with and designed convergently with the large and high-quality suite of system components created by Stallman's Project GNU and distributed by the Free Software Foundation. Because Torvalds chose to release the Linux kernel under the Free Software Foundation's General Public License, of which more below, the hundreds and eventually thousands of programmers around the world who chose to contribute their effort towards the further development of the kernel could be sure that their efforts would result in permanently free software that no one could turn into a proprietary product. Everyone knew that everyone else would be able to test, improve, and redistribute their improvements. Torvalds accepted contributions freely, and with a genially effective style maintained overall direction without dampening enthusiasm. The development of the Linux kernel proved that the Internet made it possible to aggregate collections of programmers far larger than any commercial manufacturer could afford, joined almost non-hierarchically in a development project ultimately involving more than one million lines of computer code—a scale of collaboration among geographically dispersed unpaid volunteers previously unimaginable in human history.[20]

By 1994, Linux had reached version 1.0, representing a usable production kernel. Level 2.0 was reached in 1996, and by 1998, with the kernel at 2.2.0 and available not only for x86 machines but for a variety of other machine architectures, GNU/Linux—the combination of the Linux kernel

ities of particular hardware. Once the operating system is written in a general language such as C, only that inner core, known in the trade as the kernel, will be highly specific to a particular computer architecture.

[20] A careful and creative analysis of how Torvalds made this process work, and what it implies for the social practices of creating software, was provided by Eric S. Raymond in his seminal 1997 paper, The Cathedral and the Bazaar,

http://www.tuxedo.org/~esr/writings/cathedral-bazaar/

which itself played a significant role in the expansion of the free software idea.

and the much larger body of Project GNU components—and Windows NT were the only two operating systems in the world gaining market share. A Microsoft internal assessment of the situation leaked in October 1998 and subsequently acknowledged by the company as genuine concluded that "Linux represents a best-of-breed UNIX, that is trusted in mission critical applications, and—due to it's [sic] open source code—has a long term credibility which exceeds many other competitive OS's."[21] GNU/Linux systems are now used throughout the world, operating everything from web servers at major electronic commerce sites to "ad-hoc supercomputer" clusters to the network infrastructure of money-center banks. GNU/Linux is found on the space shuttle, and running behind-the-scenes computers at (yes) Microsoft. Industry evaluations of the comparative reliability of Unix systems have repeatedly shown that Linux is far and away the most stable and reliable Unix kernel, with a reliability exceeded only by the GNU tools themselves. GNU/Linux not only out-performs commercial proprietary Unix versions for PCs in benchmarks, but is renowned for its ability to run, undisturbed and uncomplaining, for months on end in high-volume high-stress environments without crashing.

Other components of the free software movement have been equally successful. Apache, far and away the world's leading web server program, is free software, as is Perl, the programming language which is the lingua franca for the programmers who build sophisticated websites. Netscape Communications now distributes its Netscape Communicator 5.0 browser as free software, under a close variant of the Free Software Foundation's General Public License. Major PC manufacturers, including IBM, have announced plans or are already distributing GNU/Linux as a customer option on their top-of-the-line PCs intended for use as web- and fileservers. Samba, a program that allows GNU/Linux computers to act as Windows NT fileservers, is used worldwide as an alternative to Windows NT Server, and provides effective low-end competition to Microsoft in its own home market. By the standards of software quality that have been recognized in the industry for decades—and whose continuing relevance will be clear to you the next time your Windows PC crashes—the news at century's end is unambiguous. The world's most profitable and powerful corporation comes in a distant second, having excluded all but the real victor from the race. Propertarianism joined to capitalist vigor destroyed meaningful com-

[21] This is a quotation from what is known in the trade as the "Halloween memo," which can be found, as annotated by Eric Raymond, to whom it was leaked, at http://www.opensource.org/halloween1.html.

mercial competition, but when it came to making good software, anarchism won.

III Anarchism as a Mode of Production

It's a pretty story, and if only the IPdroid and the econodwarf hadn't been blinded by theory, they'd have seen it coming. But though some of us had been working for it and predicting it for years, the theoretical consequences are so subversive for the thoughtways that maintain our dwarves and droids in comfort that they can hardly be blamed for refusing to see. The facts proved that something was wrong with the "incentives" metaphor that underprops conventional intellectual property reasoning.[22] But they did more. They provided an initial glimpse into the future of human creativity in a world of global interconnection, and it's not a world made for dwarves and droids.

My argument, before we paused for refreshment in the real world, can be summarized this way: Software—whether executable programs, music, visual art, liturgy, weaponry, or what have you—consists of bitstreams, which although essentially indistinguishable are treated by a confusing multiplicity of legal categories. This multiplicity is unstable in the long term for reasons integral to the legal process. The unstable diversity of rules is caused by the need to distinguish among kinds of property interests in bitstreams. This need is primarily felt by those who stand to profit from the socially acceptable forms of monopoly created by treating ideas as property. Those of us who are worried about the social inequity and cultural hegemony created by this intellectually unsatisfying and morally repugnant regime are shouted down. Those doing the shouting, the dwarves and the droids, believe that these property rules are necessary not from any overt yearning for life in Murdochworld—though a little luxurious co-optation is always welcome—but because the metaphor of incentives, which they take to be not just an image but an argument, proves that these rules—despite their lamentable consequences—are necessary if we are to make good software. The only way to continue to believe this is to ignore the facts. At the center of the digital revolution, with the executable bit-

[22] As recently as early 1994 a talented and technically competent (though Windows-using) law and economics scholar at a major US law school confidently informed me that free software couldn't possibly exist, because no one would have any incentive to make really sophisticated programs requiring substantial investment of effort only to give them away.

streams that make everything else possible, propertarian regimes not only do not make things better, they can make things radically worse. Property concepts, whatever else may be wrong with them, do not enable and have in fact retarded progress.

But what is this mysterious alternative? Free software exists, but what are its mechanisms, and how does it generalize towards a non-propertarian theory of the digital society?

A The Legal Theory of Free Software

There is a myth, like most myths partially founded on reality, that computer programmers are all libertarians. Right-wing ones are capitalists, cleave to their stock options, and disdain taxes, unions, and civil rights laws; left-wing ones hate the market and all government, believe in strong encryption no matter how much nuclear terrorism it may cause,[23] and dislike Bill Gates because he's rich. There is doubtless a foundation for this belief. But the most significant difference between political thought inside the digirati and outside it is that in the network society, anarchism (or more properly, anti-possessive individualism) is a viable political philosophy.

The center of the free software movement's success, and the greatest achievement of Richard Stallman, is not a piece of computer code. The success of free software, including the overwhelming success of GNU/Linux, results from the ability to harness extraordinary quantities of high-quality effort for projects of immense size and profound complexity. And this ability in turn results from the legal context in which the labor is mobilized. As a visionary designer Richard Stallman created more than Emacs, GDB, or GNU. He created the General Public License.

The GPL,[24] also known as the copyleft, uses copyright, to paraphrase Toby Milsom, to counterfeit the phenomena of anarchism. As the license preamble expresses it:

> When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to

[23] This question too deserves special scrutiny, encrusted as it is with special pleading on the state-power side. See my brief essay "*So Much for Savages*: Navajo 1, Government 0 in Final Moments of Play,"
http://emoglen.law.columbia.edu/my_pubs/yu-encrypt.html

[24] See GNU General Public License, Version 2, June 1991,
http://www.fsf.org/copyleft/gpl.txt

> make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.
>
> To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.
>
> For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Many variants of this basic free software idea have been expressed in licenses of various kinds, as I have already indicated. The GPL is different from the other ways of expressing these values in one crucial respect. Section 2 of the license provides in pertinent part:

> You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work ..., provided that you also meet all of these conditions:
>
> ...
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

Section 2(b) of the GPL is sometimes called "restrictive," but its intention is liberating. It creates a commons, to which anyone may add but from which no one may subtract. Because of §2(b), each contributor to a GPL'd project is assured that she, and all other users, will be able to run, modify and redistribute the program indefinitely, that source code will always be available, and that, unlike commercial software, its longevity cannot be limited by the contingencies of the marketplace or the decisions of future developers. This "inheritance" of the GPL has sometimes been criticized as

an example of the free software movement's anti-commercial bias. Nothing could be further from the truth. The effect of §2(b) is to make commercial distributors of free software better competitors against proprietary software businesses. For confirmation of this point, one can do no better than to ask the proprietary competitors. As the author of the Microsoft "Halloween" memorandum, Vinod Vallopillil, put it:

> The GPL and its aversion to code forking reassures customers that they aren't riding an evolutionary 'dead-end' by subscribing to a particular commercial version of Linux.
>
> The "evolutionary dead-end" is the core of the software FUD argument.[25]

Translated out of Microspeak, this means that the strategy by which the dominant proprietary manufacturer drives customers away from competitors—by sowing fear, uncertainty and doubt about other software's long-term viability—is ineffective with respect to GPL'd programs. Users of GPL'd code, including those who purchase software and systems from a commercial reseller, know that future improvements and repairs will be accessible from the commons, and need not fear either the disappearance of their supplier or that someone will use a particularly attractive improvement or a desperately necessary repair as leverage for "taking the program private."

This use of intellectual property rules to create a commons in cyberspace is the central institutional structure enabling the anarchist triumph. Ensuring free access and enabling modification at each stage in the process means that the evolution of software occurs in the fast Lamarckian mode: each favorable acquired characteristic of others' work can be directly inherited. Hence the speed with which the Linux kernel, for example, outgrew all of its proprietary predecessors. Because defection is impossible, free riders are welcome, which resolves one of the central puzzles of collective action in a propertarian social system.

Non-propertarian production is also directly responsible for the famous stability and reliability of free software, which arises from what Eric Raymond calls "Linus' law": With enough eyeballs, all bugs are shallow. In practical terms, access to source code means that if I have a problem I can

[25] V. Vallopillil, Open Source Software: A (New?) Development Methodology, http://www.opensource.org/halloween1.html

fix it. Because I can fix it, I almost never have to, because someone else has almost always seen it and fixed it first.

For the free software community, commitment to anarchist production may be a moral imperative; as Richard Stallman wrote, it's about freedom, not about price. Or it may be a matter of utility, seeking to produce better software than propertarian modes of work will allow. From the droid point of view, the copyleft represents the perversion of theory, but better than any other proposal over the past decades it resolves the problems of applying copyright to the inextricably merged functional and expressive features of computer programs. That it produces better software than the alternative does not imply that traditional copyright principles should now be prohibited to those who want to own and market inferior software products, or (more charitably) whose products are too narrow in appeal for communal production. But our story should serve as a warning to droids: The world of the future will bear little relation to the world of the past. The rules are now being bent in two directions. The corporate owners of "cultural icons" and other assets who seek ever-longer terms for corporate authors, converting the "limited Time" of Article I, §8 into a freehold have naturally been whistling music to the android ear.[26] After all, who bought the droids their concert tickets? But as the propertarian position seeks to embed itself ever more strongly, in a conception of copyright liberated from the minor annoyances of limited terms and fair use, at the very center of our "cultural software" system, the anarchist counter-strike has begun. Worse is yet to befall the droids, as we shall see. But first, we must pay our final devoirs to the dwarves.

B Because It's There: Faraday's Magnet and Human Creativity

After all, they deserve an answer. Why do people make free software if they don't get to profit? Two answers have usually been given. One is half-right and the other is wrong, but both are insufficiently simple.

The wrong answer is embedded in numerous references to "the hacker gift-exchange culture." This use of ethnographic jargon wandered into the field some years ago and became rapidly, if misleadingly, ubiquitous. It reminds us only that the econometricians have so corrupted our thought

[26]The looming expiration of Mickey Mouse's ownership by Disney requires, from the point of view of that wealthy "campaign contributor," for example, an alteration of the general copyright law of the United States. See "Not Making it Any More? Vaporizing the Public Domain," in *The Invisible Barbecue*, forthcoming.

processes that any form of non-market economic behavior seems equal to every other kind. But gift-exchange, like market barter, is a propertarian institution. Reciprocity is central to these symbolic enactments of mutual dependence, and if either the yams or the fish are short-weighted, trouble results. Free software, at the risk of repetition, is a commons: no reciprocity ritual is enacted there. A few people give away code that others sell, use, change, or borrow wholesale to lift out parts for something else. Notwithstanding the very large number of people (tens of thousands, at most) who have contributed to GNU/Linux, this is orders of magnitude less than the number of users who make no contribution whatever.[27]

A part of the right answer is suggested by the claim that free software is made by those who seek reputational compensation for their activity. Famous Linux hackers, the theory is, are known all over the planet as programming deities. From this they derive either enhanced self-esteem or indirect material advancement.[28] But the programming deities, much as they have contributed to free software, have not done the bulk of the work. Reputations, as Linus Torvalds himself has often pointed out, are made by willingly acknowledging that it was all done by someone else. And, as many observers have noted, the free software movement has also produced superlative documentation. Documentation-writing is not what hackers do to attain cool, and much of the documentation has been written by people who didn't write the code. Nor must we limit the indirect material advantages of authorship to increases in reputational capital. Most free software authors I know have day jobs in the technology industries, and the skills they hone in the more creative work they do outside the market no doubt sometimes measurably enhance their value within it. And as the free software products gained critical mass and became the basis of a whole new

[27] A recent industry estimate puts the number of Linux systems worldwide at 7.5 million. See Josh McHugh, Linux: The Making of a Global Hack, Forbes, August 10, 1998.
http://www.forbes.com/forbes/98/0810/6203094s1.htm
Because the software is freely obtainable throughout the net, there is no simple way to assess actual usage.

[28] Eric Raymond is a partisan of the "ego boost" theory, to which he adds another faux-ethnographic comparison, of free software composition to the Kwakiutl potlatch. See Eric S. Raymond, Homesteading the Noosphere.
http://www.tuxedo.org/~esr/writings/homesteading .
But the potlatch, certainly a form of status competition, is unlike free software for two fundamental reasons: it is essentially hierarchical, which free software is not, and, as we have known since Thorstein Veblen first called attention to its significance, it is a form of conspicuous waste. See Thorstein Veblen, *The Theory of the Leisure Class* (New York: Viking, 1967), (1st ed. 1899), 75. These are precisely the grounds which distinguish the anti-hierarchical and utilitarian free software culture from its propertarian counterparts.

set of business models built around commercial distribution of that which people can also get for nothing, an increasing number of people are specifically employed to write free software. But in order to be employable in the field, they must already have established themselves there. Plainly, then, this motive is present, but it isn't the whole explanation.

Indeed, the rest of the answer is just too simple to have received its due. The best way to understand is to follow the brief and otherwise unsung career of an initially-grudging free software author. Microsoft's Vinod Vallopillil, in the course of writing the competitive analysis of Linux that was leaked as the second of the famous "Halloween memoranda," bought and installed a Linux system on one of his office computers. He had trouble because the (commercial) Linux distribution he installed did not contain a daemon to handle the DHCP protocol for assignment of dynamic IP addresses. The result was important enough for us to risk another prolonged exposure to the Microsoft Writing Style:

> A small number of web sites and FAQs later, I found an FTP site with a Linux DHCP client. The DHCP client was developed by an engineer employed by Fore Systems (as evidenced by his email address; I believe, however, that it was developed in his own free time). A second set of documentation/manuals was written for the DHCP client by a hacker in *Hungary* which provided relatively simple instructions on how to install/load the client.
>
> I downloaded & uncompressed the client and typed two simple commands:
>
> Make - compiles the client binaries
>
> Make Install -installed the binaries as a Linux Daemon
>
> Typing "DHCPCD" (for DHCP Client Daemon) on the command line triggered the DHCP discovery process and voila, I had IP networking running.
>
> Since I had just downloaded the DHCP client code, on an impulse I played around a bit. Although the client wasn't as extensible as the DHCP client we are shipping in NT5 (for example, it won't query for arbitrary options & store results), it was obvious how I could write the additional code to implement this functionality. The full client consisted of about 2600 lines of code.
>
> One example of esoteric, extended functionality that was clearly patched in by a third party was a set of routines to that

> would pad the DHCP request with host-specific strings required by Cable Modem / ADSL sites.
>
> A few other steps were required to configure the DHCP client to auto-start and auto-configure my Ethernet interface on boot but these were documented in the client code and in the DHCP documentation from the Hungarian developer.
>
> I'm a poorly skilled UNIX programmer but it was immediately obvious to me how to incrementally extend the DHCP client code (the feeling was exhilarating and addictive).
>
> Additionally, due directly to GPL + having the full development environment in front of me, I was in a position where I could write up my changes and email them out within a couple of hours (in contrast to how things like this would get done in NT). Engaging in that process would have prepared me for a larger, more ambitious Linux project in the future.[29]

"The feeling was exhilarating and addictive." Stop the presses: Microsoft experimentally verifies Moglen's Metaphorical Corollary to Faraday's Law. Wrap the Internet around every brain on the planet and spin the planet. Software flows in the wires. It's an emergent property of human minds to create. "Due directly to the GPL," as Vallopillil rightly pointed out, free software made available to him an exhilarating increase in his own creativity, of a kind not achievable in his day job working for the Greatest Programming Company on Earth. If only he had emailed that first addictive fix, who knows where he'd be now?

So, in the end, my dwarvish friends, it's just a human thing. Rather like why Figaro sings, why Mozart wrote the music for him to sing to, and why we all make up new words: Because we can. Homo ludens, meet Homo faber. The social condition of global interconnection that we call the Internet makes it possible for all of us to be creative in new and previously undreamed-of ways. Unless we allow "ownership" to interfere. Repeat after me, ye dwarves and men: Resist the resistance!

[29] Vinod Vallopillil, Linux OS Competitive Analysis (Halloween II).
http://www.opensource.org/halloween2.html
Note Vallopillil's surprise that a program written in California had been subsequently documented by a programmer in Hungary.

IV Their Lordships Die in the Dark?

For the IPdroid, fresh off the plane from a week at Bellagio paid for by Dreamworks SKG, it's enough to cause indigestion.

Unlock the possibilities of human creativity by connecting everyone to everyone else? Get the ownership system out of the way so that we can all add our voices to the choir, even if that means pasting our singing on top of the Mormon Tabernacle and sending the output to a friend? No one sitting slack-jawed in front of a televised mixture of violence and imminent copulation carefully devised to heighten the young male eyeball's interest in a beer commercial? What will become of civilization? Or at least of copyrights teachers?

But perhaps this is premature. I've only been talking about software. Real software, the old kind, that runs computers. Not like the software that runs DVD players, or the kind made by the Grateful Dead. "Oh yes, the Grateful Dead. Something strange about them, wasn't there? Didn't prohibit recording at their concerts. Didn't mind if their fans rather riled the recording industry. Seem to have done all right, though, you gotta admit. Senator Patrick Leahy, isn't he a former Deadhead? I wonder if he'll vote to extend corporate authorship terms to 125 years, so that Disney doesn't lose The Mouse in 2004. And those DVD players—they're computers, aren't they?"

In the digital society, it's all connected. We can't depend for the long run on distinguishing one bitstream from another in order to figure out which rules apply. What happened to software is already happening to music. Their recording industry lordships are now scrambling wildly to retain control over distribution, as both musicians and listeners realize that the middlepeople are no longer necessary. The Great Potemkin Village of 1999, the so-called Secure Digital Music Initiative, will have collapsed long before the first Internet President gets inaugurated, for simple technical reasons as obvious to those who know as the ones that dictated the triumph of free software.[30] The anarchist revolution in music is different from the one in software *tout court*, but here too—as any teenager with an MP3 collection of self-released music from unsigned artists can tell you—theory has been killed off by the facts. Whether you are Mick Jagger, or a great national artist from the third world looking for a global audience, or a garret-

[30]See "They're Playing Our Song: The Day the Music Industry Died," in *The Invisible Barbecue*, forthcoming.

dweller reinventing music, the recording industry will soon have nothing to offer you that you can't get better for free. And music doesn't sound worse when distributed for free, pay what you want directly to the artist, and don't pay anything if you don't want to. Give it to your friends; they might like it.

What happened to music is also happening to news. The wire services, as any US law student learns even before taking the near-obligatory course in Copyright for Droids, have a protectible property interest in their expression of the news, even if not in the facts the news reports.[31] So why are they now giving all their output away? Because in the world of the net, most news is commodity news. And the original advantage of the news gatherers, that they were internally connected in ways others were not when communications were expensive, is gone. Now what matters is collecting eyeballs to deliver to advertisers. It isn't the wire services that have the advantage in covering Kosovo, that's for sure. Much less those paragons of "intellectual" property, their television lordships. They, with their overpaid pretty people and their massive technical infrastructure, are about the only organizations in the world that can't afford to be everywhere all the time. And then they have to limit themselves to ninety seconds a story, or the eyeball hunters will go somewhere else. So who makes better news, the propertarians or the anarchists? We shall soon see.

Oscar Wilde says somewhere that the problem with socialism is that it takes up too many evenings. The problems with anarchism as a social system are also about transaction costs. But the digital revolution alters two aspects of political economy that have been otherwise invariant throughout human history. All software has zero marginal cost in the world of the net, while the costs of social coordination have been so far reduced as to permit the rapid formation and dissolution of large-scale and highly diverse social groupings entirely without geographic limitation.[32] Such fundamental change in the material circumstances of life necessarily produces equally fundamental changes in culture. Think not? Tell it to the Iroquois. And of course such profound shifts in culture are threats to existing power relations. Think not? Ask the Chinese Communist Party. Or wait twenty-five years and see if you can find them for purposes of making the inquiry.

[31] International News Service v. Associated Press, 248 U.S. 215 (1918). With regard to the actual terse, purely functional expressions of breaking news actually at stake in the jostling among wire services, this was always a distinction only a droid could love.

[32] See "No Prodigal Son: The Political Theory of Universal Interconnection," in *The Invisible Barbecue*, forthcoming.

In this context, the obsolescence of the IPdroid is neither unforseeable nor tragic. Indeed it may find itself clanking off into the desert, still lucidly explaining to an imaginary room the profitably complicated rules for a world that no longer exists. But at least it will have familiar company, recognizable from all those glittering parties in Davos, Hollywood, and Brussels. Our Media Lords are now at handigrips with fate, however much they may feel that the Force is with them. The rules about bitstreams are now of dubious utility for maintaining power by co-opting human creativity. Seen clearly in the light of day, these Emperors have even fewer clothes than the models they use to grab our eyeballs. Unless supported by user-disabling technology, a culture of pervasive surveillance that permits every reader of every "property" to be logged and charged, and a smokescreen of droid-breath assuring each and every young person that human creativity would vanish without the benevolent aristocracy of BillG the Creator, Lord Murdoch of Everywhere, the Spielmeister and the Lord High Mouse, their reign is nearly done. But what's at stake is the control of the scarcest resource of all: our attention. Conscripting that makes all the money in the world in the digital economy, and the current lords of the earth will fight for it. Leagued against them are only the anarchists: nobodies, hippies, hobbyists, lovers, and artists. The resulting unequal contest is the great political and legal issue of our time. Aristocracy looks hard to beat, but that's how it looked in 1788 and 1913 too. It is, as Chou En-Lai said about the meaning of the French Revolution, too soon to tell.

References

Balkin, J. M., *Cultural Software: a Theory of Ideology* (New Haven: Yale University Press, 1998).

Berlin, Isaiah, *The Hedgehog and the Fox; an Essay on Tolstoy's View of History* (New York: Simon and Schuster, 1953).

Maine, Henry Sumner, *Ancient Law: Its Connection with the Early History of Society, and its Relation to Modern Ideas*, 1st edn. (London: J. Murray, 1861).

Milsom, S. F. C., *Historical Foundations of the Common Law*, 2nd edn. (London: Butterworths, 1981).

Veblen, Thorstein, *The Theory of the Leisure Class* (New York: Viking, 1967).

Part III

Community Initiatives: Working and Living Together

Chapter 11

Contributor Covenant Overview (Coraline Ada Emkhe)

Contributor Covenant

A Code of Conduct for Open Source Projects

Open Source has always been a foundation of the Internet, and with the advent of social open source networks this is more true than ever. But free, libre, and open source projects suffer from a startling lack of diversity, with dramatically low representation by women, people of color, and other marginalized populations.

Often it is the unintentional assumptions and actions of project maintainers and participants that make open source projects unwelcoming (or even hostile) to marginalized people: making assumptions about gender or race, reinforcing stereotypes, using sexualized or otherwise inappropriate language, or demonstrating a lack of regard for the safety and well-being of vulnerable people.

One way to begin addressing this problem is to be overt in our openness, welcoming all people to contribute, and pledging in return to value them as whole human beings and

to foster an atmosphere of kindness, cooperation, and understanding.

Adopting the Contributor Covenant can be one way to express and codify these values and signal your intention to make your open source community welcoming, diverse, and inclusive.

Contributor Covenant v1.4.1

You can view and download the latest version of the Contributor Covenant here:

- English (Markdown version)
- English (HTML version)
- English (text version)

For translations of the Contributor Covenant, please see our translations page.

The Contributor Covenant uses semantic versioning for revisions so all URLs are permanent. Previous versions are available here: 1.0, 1.1, 1.2, and 1.3.

Using the Contributor Covenant

We recommend that you add the Markdown or text version

of the Contributor Covenant to your source code repository at the root level.

Thanks to Simon Vansintjan there is an automated way to add Contributor Covenant to your project. Assuming that you have Node.js installed, simply run the following two commands from your project folder:

```
npm install -g covgen covgen <your_email_address>
```

If you have npm 5.x installed you can run `npx covgen <your_email_address>` instead of installing globally.

For subsequent projects, simply repeat the second command.

You may want to add language similar to this to introduce your code of conduct:

> Please note that this project is released with a Contributor Code of Conduct. By participating in this project you agree to abide by its terms.

You may also use the permalinks given above to reference from your project home page.

Important! You must add a contact method to the placeholder in the document so that people know how to report violations.

If you are using a markdown README file in your source

code repository, you may want to add a badge like this one 

using the code below.

```
[![Contributor Covenant](https://img.shields.io/badge
```

*The Contributor Covenant is released under the **Creative Commons Attribution 4.0 International Public License**, which requires that attribution be included.*

Enforcing the Contributor Covenant

> Morality cannot be legislated, but behavior can be regulated.
>
> *— Dr. Martin Luther King, Jr.*

Do not simply add the Contributor Covenant to your project and assume that any problems with civility, harassment, or discrimination will be solved. As a project maintainer you must be committed to enforcing the code of conduct. A code of conduct without enforcement sends a false signal that your project is welcoming and inclusive, and can create a dangerous situation for marginalized people who participate. Adding the Contributor Covenant to a project places responsibility on the project team that must not be taken lightly.

Before adopting the Contributor Covenant take the time to discuss and decide how to deal with problems as they

emerge. Document the policy and procedure for enforcement, and add it to your README or in another visible, appropriate place. Consider if your project team has the willingness and maturity to follow through on your enforcement procedures.

Some resources useful for thinking about enforcement:

- Community Safety and Accountability
- Enforcing Your Code of Conduct: Effective Incident Response
- Django Code of Conduct Enforcement Manual
- jQuery Foundation Code of Conduct Enforcement Manual
- How Mozilla is Making Code of Conduct Enforcement Real - and Scaling It

Adopters of the Contributor Covenant

This code of conduct has already been adopted by over 200,000 open source projects. Here are just a few major projects and organizations using the Contributor Covenant.

Atom
AngularJS
Babel
Bootstrap
Bundler
chef-rvm

Cloud Native Compute Fou...
CocoaPods
Creative Commons
Cucumber
Crystal
curl
Diaspora
Discourse
Eclipse
Electron
Elixir
Exercism.io
Gatsby
GitLab
Golang
Google
Homebrew-Cask
Intel OTC
Jekyll
Jenkins
JRuby
Hanami
Kong
Kubernetes
Linux
Metasploit Framework
Mono
Mozilla Webmaker
.NET Foundation
Rails
rbenv
React
ROM
RSpec
ruby-community
rubygems
RubyGems.org
RVM
Salesforce OSS
Shoes
Spring
Swift
Symfony
Target
TensorFlow
Travis CI
Twilio
Visual F#

Vue.js Yarn

See this page for more.

To add your project to the list, submit a pull request.

How to Contribute

The Contributor Covenant is a living document, and has been open sourced. Contributions in the form of issues and pull requests are welcomed and encouraged.

Chapter 12

Contributor Covenant Code of Conduct (Coraline Ada Emkhe)

Contributor Covenant

CONTRIBUTOR COVENANT CODE OF CONDUCT

Our Pledge

In the interest of fostering an open and welcoming environment, we as contributors and maintainers pledge to make participation in our project and our community a harassment-free experience for everyone, regardless of age, body size, disability, ethnicity, sex characteristics, gender identity and expression, level of experience, education, socio-economic status, nationality, personal appearance, race, religion, or sexual identity and orientation.

Our Standards

Examples of behavior that contributes to creating a positive environment include:

- Using welcoming and inclusive language

- Being respectful of differing viewpoints and experiences
- Gracefully accepting constructive criticism
- Focusing on what is best for the community
- Showing empathy towards other community members

Examples of unacceptable behavior by participants include:

- The use of sexualized language or imagery and unwelcome sexual attention or advances
- Trolling, insulting/derogatory comments, and personal or political attacks
- Public or private harassment
- Publishing others' private information, such as a physical or electronic address, without explicit permission
- Other conduct which could reasonably be considered inappropriate in a professional setting

Our Responsibilities

Project maintainers are responsible for clarifying the standards of acceptable behavior and are expected to take appropriate and fair corrective action in response to any instances of unacceptable behavior.

Project maintainers have the right and responsibility to remove, edit, or reject comments, commits, code, wiki edits, issues, and other contributions that are not aligned to this

Code of Conduct, or to ban temporarily or permanently any contributor for other behaviors that they deem inappropriate, threatening, offensive, or harmful.

Scope

This Code of Conduct applies within all project spaces, and it also applies when an individual is representing the project or its community in public spaces. Examples of representing a project or community include using an official project e-mail address, posting via an official social media account, or acting as an appointed representative at an online or offline event. Representation of a project may be further defined and clarified by project maintainers.

Enforcement

Instances of abusive, harassing, or otherwise unacceptable behavior may be reported by contacting the project team at [INSERT EMAIL ADDRESS]. All complaints will be reviewed and investigated and will result in a response that is deemed necessary and appropriate to the circumstances. The project team is obligated to maintain confidentiality with regard to the reporter of an incident. Further details of specific enforcement policies may be posted separately.

Project maintainers who do not follow or enforce the Code

of Conduct in good faith may face temporary or permanent repercussions as determined by other members of the project's leadership.

Attribution

This Code of Conduct is adapted from the Contributor Covenant, version 1.4, available at https://www.contributor-covenant.org/version/1/4/code-of-conduct.html

For answers to common questions about this code of conduct, see https://www.contributor-covenant.org/faq

Chapter 13

Linux Kernel Contributor Covenant Code of Conduct Interpretation

Linux Kernel Contributor Covenant Code of Conduct Interpretation

The Contributor Covenant Code of Conduct is a general document meant to provide a set of rules for almost any open source community. Every open-source community is unique and the Linux kernel is no exception. Because of this, this document describes how we in the Linux kernel community will interpret it. We also do not expect this interpretation to be static over time, and will adjust it as needed.

The Linux kernel development effort is a very personal process compared to "traditional" ways of developing software. Your contributions and ideas behind them will be carefully reviewed, often resulting in critique and criticism. The review will almost always require improvements before the material can be included in the kernel. Know that this happens because everyone involved wants to see the best possible solution for the overall success of Linux. This development process has been proven to create the most robust operating system kernel ever, and we do not want to do anything to cause the quality of submission and eventual result to ever decrease.

Maintainers

The Code of Conduct uses the term "maintainers" numerous times. In the kernel community, a "maintainer" is anyone who is responsible for a subsystem, driver, or file, and is listed in the MAINTAINERS file in the kernel source tree.

Responsibilities

The Code of Conduct mentions rights and responsibilities for maintainers, and this needs some further clarifications.

First and foremost, it is a reasonable expectation to have maintainers lead by example.

That being said, our community is vast and broad, and there is no new requirement for maintainers to unilaterally handle how other people behave in the parts of the community where they are active. That responsibility is upon all of us, and ultimately the Code of Conduct documents final escalation paths in case of unresolved concerns regarding conduct issues.

Maintainers should be willing to help when problems occur, and work with others in the community when needed. Do not be afraid to reach out to the Technical Advisory Board (TAB) or other maintainers if you're uncertain how to handle situations that come up. It will not be considered a violation report unless you want it to be. If you are uncertain about approaching the TAB or any other maintainers, please reach out to our conflict mediator, Mishi Choudhary <mishi@linux.com>.

In the end, "be kind to each other" is really what the end goal is for everybody. We know everyone is human and we all fail at times, but the primary goal for all of us should be to work toward amicable resolutions of problems. Enforcement of the code of conduct will only be a last resort option.

Our goal of creating a robust and technically advanced operating system and the technical complexity involved naturally require expertise and decision-making.

The required expertise varies depending on the area of contribution. It is determined mainly by context and technical complexity and only secondary by the expectations of contributors and maintainers.

Both the expertise expectations and decision-making are subject to discussion, but at the very end there is a basic necessity to be able to make decisions in order to make progress. This prerogative is in the hands of maintainers and project's leadership and is expected to be used in good faith.

As a consequence, setting expertise expectations, making decisions and rejecting unsuitable contributions are not viewed as a violation of the Code of Conduct.

While maintainers are in general welcoming to newcomers, their capacity of helping contributors overcome the entry hurdles is limited, so they have to set priorities. This, also, is not to be seen as a violation of the Code of Conduct. The kernel community is aware of that and provides entry level programs in various forms like kernelnewbies.org.

Scope

The Linux kernel community primarily interacts on a set of public email lists distributed around a number of different servers controlled by a number of different companies or individuals. All of these lists are defined in the MAINTAINERS file in the kernel source tree. Any emails sent to those mailing lists are considered covered by the Code of Conduct.

Developers who use the kernel.org bugzilla, and other subsystem bugzilla or bug tracking tools should follow the guidelines of the Code of Conduct. The Linux kernel community does not have an "official" project email address, or "official" social media

address. Any activity performed using a kernel.org email account must follow the Code of Conduct as published for kernel.org, just as any individual using a corporate email account must follow the specific rules of that corporation.

The Code of Conduct does not prohibit continuing to include names, email addresses, and associated comments in mailing list messages, kernel change log messages, or code comments.

Interaction in other forums is covered by whatever rules apply to said forums and is in general not covered by the Code of Conduct. Exceptions may be considered for extreme circumstances.

Contributions submitted for the kernel should use appropriate language. Content that already exists predating the Code of Conduct will not be addressed now as a violation. Inappropriate language can be seen as a bug, though; such bugs will be fixed more quickly if any interested parties submit patches to that effect. Expressions that are currently part of the user/kernel API, or reflect terminology used in published standards or specifications, are not considered bugs.

Enforcement

The address listed in the Code of Conduct goes to the Code of Conduct Committee. The exact members receiving these emails at any given time are listed at https://kernel.org/code-of-conduct.html. Members can not access reports made before they joined or after they have left the committee.

The initial Code of Conduct Committee consists of volunteer members of the TAB, as well as a professional mediator acting as a neutral third party. The first task of the committee is to establish documented processes, which will be made public.

Any member of the committee, including the mediator, can be contacted directly if a reporter does not wish to include the full committee in a complaint or concern.

The Code of Conduct Committee reviews the cases according to the processes (see above) and consults with the TAB as needed and appropriate, for instance to request and receive information about the kernel community.

Any decisions by the committee will be brought to the TAB, for implementation of enforcement with the relevant maintainers if needed. A decision by the Code of Conduct Committee can be overturned by the TAB by a two-thirds vote.

At quarterly intervals, the Code of Conduct Committee and TAB will provide a report summarizing the anonymised reports that the Code of Conduct committee has received and their status, as well details of any overridden decisions including

complete and identifiable voting details.

We expect to establish a different process for Code of Conduct Committee staffing beyond the bootstrap period. This document will be updated with that information when this occurs.

Chapter 14

Linux Foundation Code of Conduct

The Linux Foundation and its Projects are dedicated to providing a harassment-free experience for participants at all of our events. Linux Foundation (and LF Project) events are working conferences intended for professional networking and collaboration in the Linux and greater open source communities. They exist to encourage the open exchange of ideas and expression and require an environment that recognizes the inherent worth of every person and group. While at Linux Foundation (or LF Project) events or related ancillary or social events, any participants, including speakers, attendees, volunteers, sponsors, exhibitors, booth staff and anyone else, should not engage in harassment in any form.

Expected Behavior

All event participants are expected to behave in accordance with professional standards, with both the Linux Foundation Code of Conduct as well as their respective employer's policies governing appropriate workplace behavior, and applicable laws

Unacceptable Behavior

Harassment will not be tolerated in any form, including but not limited to harassment based on gender, gender identity and expression, sexual orientation, disability, physical appearance, body size, race, age, religion or any other status protected by laws in which the conference or program is being held. Harassment includes the use of abusive, offensive or degrading language, intimidation, stalking, harassing photography or recording, inappropriate physical contact, sexual imagery and unwelcome sexual advances or requests for sexual favors. Any report of harassment at one of our events will be addressed immediately. Participants asked to stop any harassing behavior are expected to comply immediately. Anyone who witnesses or is subjected to unacceptable behavior should notify a conference

Exhibitors should not use sexualized images, activities, or other material in their booths and must refrain from the use of sexualized clothing/uniforms/costumes, or otherwise creating a sexualized environment. Speakers should not use sexual language, images, or any language or images that would constitute harassment as defined above in their talks.

Consequences of Unacceptable Behavior

If a participant engages in harassing behavior, the conference organizers may take any action they deem appropriate, ranging from issuance of a warning to the offending individual to expulsion from the conference with no refund, depending on the circumstances The Linux Foundation (and LF Projects) reserve the right to exclude any participant found to be engaging in harassing behavior from participating in any further Linux Foundation (or LF Project) events, trainings or other activities.

What To Do If You Witness Or Are Subject To Unacceptable Behavior

If you are being harassed, notice that someone else is being harassed, or have any other concerns relating to harassment, please contact a member of event staff immediately. Event staff can be identified by t-shirts/staff badges onsite; and an organizer can be found at the event registration counter at any time. You are also encouraged to contact Angela Brown, VP of Events at angela (at) linuxfoundation (dot) org with any questions or concerns.

Incident Response

Our staff has has had incident response training and responds to harassment reports and does so in accordance with the process recommended by the Ada Initiative, which can be found here on the Geek Feminism Wiki. As referenced above, if a participant engages in harassing behavior, the conference organizers may take any action they deem appropriate, ranging from issuance of a warning to the offending individual to expulsion from the conference with no refund, depending on the circumstances The Linux Foundation (and LF Projects) reserve the right to exclude any participant found to be engaging in harassing behavior from participating in any further Linux Foundation (or LF Project) events, trainings

Conference staff will also provide support to victims, including, but not limited to:

- Providing an escort
- Contacting hotel/venue security or local law enforcement
- Briefing key event staff to for response/victim assistance
- And otherwise assisting those experiencing harassment to ensure that they feel safe for the duration of the conference.

Pre-Event Concerns

If you are planning to attend an upcoming event, and have concerns regarding another individual who may be present, please contact Angela Brown, VP of Events at angela (at) linuxfoundation (dot) org. Precautions will be taken to ensure a victim's comfort and safety, including, but not limited to: providing an escort, prepping onsite event staff, keeping victim and harasser from attending the same talks/social events and providing onsite contact cell phone numbers for immediate contact.

Chapter 15

Linux Foundation and RISC-V Foundation Announce Joint Collaboration

The Linux Foundation and RISC-V Foundation Announce Joint Collaboration to Enable a New Era of Open Architecture

By The Linux Foundation | November 27, 2018

RISC-V Foundation to leverage the Linux Foundation's tools infrastructure, services and training programs

SAN FRANCISCO and BERKELEY, CA – Nov. 27, 2018 –The Linux Foundation, the nonprofit organization enabling mass innovation through open source, and the RISC-V Foundation, a non-profit corporation controlled by its members to drive the adoption and implementation of the free and open RISC-V instruction set architecture (ISA), today announced a joint collaboration agreement to accelerate open source development and adoption of the RISC-V ISA.

The RISC-V Foundation includes over 210 institutional, academic and individual members from around the world and has realized 100 percent year-over-year membership growth. This partnership with the Linux Foundation will enable the RISC-V Foundation to grow the RISC-V ecosystem with improved support for the development of new applications and architectures across all computing platforms.

"With the rapid international adoption of the RISC-V ISA, we need increased scale and resources to support the explosive growth of the RISC-V ecosystem. The Linux Foundation is an ideal partner given the open source nature of both organizations," said Rick O'Connor, executive director of the non-profit RISC-V Foundation. "This joint collaboration with the Linux Foundation will enable the RISC-V Foundation to offer more robust support and educational tools for the active RISC-V community,

"RISC-V has great traction in a number of markets with applications for AI, machine learning, IoT, augmented reality, cloud, data centers, semiconductors, networking and more. RISC-V is a technology that has the potential to greatly advance open hardware architecture," said Jim Zemlin, executive director at the Linux Foundation. "We look forward to collaborating with the RISC-V Foundation to advance RISC-V ISA adoption and build a strong ecosystem globally."

Since its inception in 2015, RISC-V has quickly evolved its ecosystem to feature leading technology companies and emerging startups all working together to enable a wide range of open-source and proprietary RISC-V hardware and software solutions. Members are solving some of today's most complex design challenges including security, performance, power, efficiency, flexibility and more.

In addition to neutral governance and best practices for open source development, The Linux Foundation will also provide an influx of resources for the RISC-V ecosystem, such as training programs, infrastructure tools, as well as community outreach, marketing and legal expertise.

The RISC-V ISA offers a number of advantages over other architectures, including its openness, simplicity, clean-slate design, modularity, extensibility and stability, delivering a new level of software and hardware freedom on architecture.

The Linux Foundation and the RISC-V communities are already collaborating on a pair of "Getting Started" guides for running the Zephyr, a small, scalable open source RTOS for connected, resource constrained devices, and Linux operating systems on RISC-V based platforms. The Zephyr and Linux guides will be unveiled at the RISC-V Summit on Dec. 3, 2018, in Santa Clara during training classes led by project contributors from RISC-V Foundation Founding Platinum Members Antmicro, Google, Microchip Technology and Western Digital, in addition to the Linux Foundation. For further details regarding the RISC-V Summit, please visit https://tmt.knect365.com/risc-v-summit/.

About RISC-V Foundation

RISC-V (pronounced "risk-five") is a free and open ISA enabling a new era of

collaborative community of software and hardware innovators powering a new era of processor innovation. Born in academia and research, RISC-V ISA delivers a new level of free, extensible software and hardware freedom on architecture, paving the way for the next 50 years of computing design and innovation.

The RISC-V Foundation, a non-profit corporation controlled by its members, directs the future development and drives the adoption of the RISC-V ISA. Members of the RISC-V Foundation have access to and participate in the development of the RISC-V ISA specifications and related HW / SW ecosystem. More information can be found at www.riscv.org.

About the Linux Foundation

The Linux Foundation is the organization of choice for the world's top developers and companies to build ecosystems that accelerate open technology development and industry adoption. Together with the worldwide open source community, it is solving the hardest technology problems by creating the largest shared technology investment in history. Founded in 2000, The Linux Foundation today provides tools, training and events to scale any open source project, which together deliver an economic impact not achievable by any one company. More information can be found at www.linuxfoundation.org.

# # #

Chapter 16

Intel, Linux Launch Open Source Silicon Groups

RISC-V SPECIFICATIONS

- Unprivileged Specification (/specifications/)
- Privileged ISA Specification (/specifications/privileged-isa)
- Debug Specification (/specifications/debug-specification/)

RISC-V SOFTWARE

- Software Status (/software-status/)

RISC-V CORES

NEWS (HTTPS://RISCV.ORG/CATEGORY/NEWS/)

SDxCentral Article: Intel, Linux Foundation Launch Open Source Silicon Groups

DATE: MARCH 14, 2019

Two new open source silicon groups, one led by Linux Foundation and the other by Intel, launched this week.

The Linux Foundation on Monday announced its new CHIPS (Common Hardware for Interfaces, Processors and Systems) Alliance with member companies **Google (https://about.google/intl/en_US/)**, **Western Digital (https://www.wd.com/about-wd.html)**, **Esperanto Technologies (http://www.esperantotech.com/)**, and **SiFive (https://www.sifive.com/)**. On the same day tech heavyweights Intel, **Alibaba (https://www.alibabagroup.com/en/global/home)**, Cisco, Dell EMC, Facebook, Google, Hewlett Packard Enterprise (HPE), **Huawei (https://www.huawei.com/us/)**, and Microsoft formed a consortium to

- **RISC-V Cores (/risc-v-cores/)**

develop open interconnect technology called Compute Express Link (CXL).

The foundation for the CHIPS Alliance — the open RISC-V (pronounced "risk-five") architecture — started as a separate organization in 2016 before being handed off to the Linux Foundation. It's an open source hardware instruction set architecture (ISA) based on established reduced instruction set computer (RISC) principles. In also includes supporting software. "But it does not specify the actual implementation of a RISC-V compute, so potential architectures range from small, IoT devices to big data center processors," Bandic said. Western Digital is also a co-founder of RISC-V. "The best analogy would be the common Linux OS for all the computers in data centers today, with every possible detail of source code known and documented."

To read more, please visit: **https://www.sdxcentral.com/articles/news/intel-linux-foundation-launch-open-source-silicon-groups/2019/03/ (https://www.sdxcentral.com/articles/news/intel-linux-foundation-launch-open-source-silicon-groups/2019/03/)**.

TAGS:

/workshops /proceedings/)

- **RISC-V Foundation Community Code of Conduct (https://riscv.org /risc-v-foundation-community-code-of-conduct/)**

- **RISC-V Software Developers (/mailing-lists/)**

Privacy Policy (/privacy-policy/)

Chapter 17

A Survey of Open Processor Core Licensing
(Andrew Katz

A Survey of Open Processor Core Licensing

Andrew Katz,[a]

(a) Partner, Moorcrofts LLP

DOI: 10.5033/ifosslr.v10i1.130

Abstract
In the Spring of 2018, Western Digital Corporation commissioned Andrew Katz of Moorcrofts LLP to prepare a survey of open processor core licensing. This is an edited version of that report.

Keywords
Law; information technology; Free and Open Source Software; open hardware licensing; processor cores

Foreword by Alan Tse, Western Digital Corporation:

Western Digital's relationship with open source has evolved significantly over the last decade. When I first joined Western Digital, our main focus was on open source compliance. That is because in 2009 we were one of the first major companies sued for our open source use. As a result, the main goal for the next few years was to prevent any litigation happening again and we viewed open source with some trepidation. Over time our view shifted as we had to learn about the importance of the open source community and how to be a good participant in that community. And over the years, we have increased our participation – not to avoid litigation, but because our own business interests have started to align. Over the years we have made multiple contributions to the Linux kernel and other open source projects and we have released internal tools that we thought others could use. Now that it has been almost a decade since that first lawsuit, we would like to think that we have learnt a bit more about the open source community and we are proud to say we are a part of that community.

While we have been public about our support of RISC-V and plans for RISC-V cores since 2017, we also believe the best way to show our commitment to the open source community is by leading from the front. Following our announcement at the December 2018 RISC-V Summit, we recently released our RISC-V SweRV Core under an Apache-2.0 licence on January 24, 2019.[1]

In deciding our licensing strategy for our core release, we engaged Andrew Katz to help us understand the community norms for open source hardware. Owing to his involvement in the drafting of two open source hardware licences, we believed he was at the forefront of Legal scholarship on this issue. His report that follows was instrumental as we balanced our goals of community growth and protection in a space with unique constraints. It's unique because open source

1 For more information see <https://github.com/westerndigitalcorporation/swerv>

hardware is a capital-intensive field quite different from software and the fact that the established open source licences were written without open source hardware in mind. We are happy to release this research to the community and hope this research and our journey serves as a beacon to our peers to join use in the open source hardware community.

– Alan Tse, Associate General Counsel, Western Digital.[2]

Introduction

The research was undertaken by Andrew Katz between March 26 and April 22 2018.[3] The methodology was as follows:

1. To identify major open hardware communities using a combination of research and pre-existing knowledge of various open hardware activities that Andrew Katz has been involved in including both specific projects and umbrella organisations.

2. To undertake research of those organisations and schedule and carry out a range of telephone interviews with identified leading individuals in the field. Given the relatively short time available to undertake the research, a total of eight individuals were identified, of whom six were able to agree to an interview within the time available for the first version of this report. A further two individuals arranged to be interviewed on a date after the original date of submission of the report to Western Digital, and their responses have been taken in to account in the updated version. No one who was approached declined to take part in the research, and all were very open and candid. We are grateful for their time and interest in the project. We also requested further input from the interviewees about community development and involvement, based on the answers to the first round of questions, and two individuals responded comprehensively by email. Their responses were taken into account in the report.

3. To review the projects listed on LibreCores and OpenCores.org, and the list researched by Mohammad Shahrad[4] and updated as a result of further desktop research and responses from interviewees.

4. The results of the research were compiled into this report.

5. In order to facilitate candour on the part of the interviewees, the interviewees were told that their names would not be linked to specific comments they made in a manner similar to the Chatham House Rule. Subsequently, the individuals kindly consented to their names being released.

6. To avoid bias in answers provided, the interviewees were told the research was being undertaken on behalf of a major US digital hardware manufacturer, but no further

2 Alan Tse is a member of Western Digital's Legal team and responsible for open source compliance across the company and supporting Western Digital's open source strategy. His practice covers product lines both up and down the stack including storage devices firmware, consumer devices, data centre systems, and now even hardware cores. As a former computer engineer who grew up using open source software and anxiously waiting for the year of the Linux desktop, he has watched the evolution of open source throughout the tech industry and occasionally dabbles in various open source communities.

3 The data presented in this paper represents information obtained during that research period, unless explicitly stated otherwise. For example, during discussions with Mohammad Shahrad (see footnotes 4, 19 and 20) we agreed to provide him with an updated of the data he presented in the paper referenced at footnote 4, and since this update was provided as at 29 January 2019, we decided to update the relevant text and appendix of this report accordingly. It does not affect the conclusions. The author thanks Heather Stewart for her invaluable assistance in the updating process.

4 Balkind, Joseph, et al. (2016) 'OpenPiton: An Open Source Manycore Research Framework', ASPLOS '16, pp 217 – 232. <http://parallel.princeton.edu/papers/openpiton-asplos16.pdf> DOI: 10.1145/2872362.2872414

information was provided about the research sponsor. The identity of the sponsor was released to the interviewees some months later when they were asked if they were prepared to waive anonymity.

Open Source Hardware and Licensing

Summary

Broad consensus is that 'Open Source Hardware' is hardware whose licensing terms comply with the definition set out by the Open Source Hardware Association. Although the thrust of the definition is relevant to this report, the detail is not.[5] The OSHWA definition follows the Open Source Initiative's definition for Open Source software licensing.[6]

Specific licences which have been identified[7] by OSHWA are:

Copyleft (reciprocal) licences:

- Creative Commons Attribution, Share-Alike (CC-BY-SA)
- GNU General Public License (GPL)
- Hardware-Specific Licenses: TAPR OHL, CERN OHL[8]

Permissive Licences

- Free BSD license (BSD-2-Clause)[9]
- MIT license (MIT)
- Creative Commons Attribution (CC-BY-3.0)[10]
- Hardware-Specific License: Solderpad Hardware Licence[11]

Given that the above licences are specifically referenced by OSHWA we can make the reasonable assumption that they meet the OSHWA definition. OSHWA does not (at the time of writing) have a process for approving licences. It can be assumed that licences (such as Apache) which are approved by the OSI would also meet the OSHWA criteria.

Licences that were identified during the course of this survey as applying to various open source hardware projects are:

5 For more information see <https://www.oshwa.org/definition/>
6 With the interesting distinction that in the preamble, OSHWA states that the design must be publicly available so that anyone can make etc. the design. OSI only requires that the licensing terms enable the licensee to make open source software publicly available, but not that public availability itself is necessary.
7 <https://www.oshwa.org/sharing-best-practices/>
8 Andrew Katz has been involved in the drafting of CERN OHL <https://www.ohwr.org/documents/294>.
9 <https://opensource.org/licenses/BSD-2-Clause>
10 <https://creativecommons.org/licenses/by/3.0/>
11 Andrew Katz drafted the Solderpad Licence. <http://solderpad.org/licenses/>

Licence	Comments
BSD-2-Clause (simple permissive)	Widely used for many types of open source hardware, including processor cores
MIT (simple permissive)	Widely used for open source hardware
ISC[12] (simple permissive)	Sometimes used for open source hardware
Apache-2.0 (permissive with patent clauses)	Widely used for open source hardware
GPLv3 (strong copyleft with patent licence)	Frequently used for open source hardware
GPLv2 (strong copyleft without patent licence)	Frequently used for open source hardware
LGPL (various versions)	Frequently used for open source hardware
MPL-2.0 (weak copyleft with patent grant)	Rarely used for open source hardware

Table 1: Open Source Software Licences

Licence	Comments
Creative Commons Attribution (various versions)	Widely used for open hardware designs
Creative Commons Share-Alike (various versions)	Widely used for open hardware designs
Creative Commons Public Domain Dedication (CC0)	Widely used for open hardware designs

Table 2: Open Content Licences

Licence	Comments
TAPR (Tucson Amateur Packet Radio) Open Hardware License	Mainly used for RF circuit boards. Has interesting copyleft mechanism, based on patents
CERN OHL (various versions)	Used for a wide variety of open hardware but originally designed mainly for applicability to circuit boards
Solderpad Licence (Versions 0.51 and 2) (an Apache-based Open Hardware License)	Used for a wide variety of hardware, including cores
Open Hardware Description Licence (Mozilla Public License-based open software licence)	Designed specifically for semiconductor cores. Rarely used.
NVDIA Open NVDLA License and Agreement v1 (an Apache-based Open Hardware License)	Designed specifically for NVDLA (Nvidia Deep Learning Accelerator)

Table 3: Hardware Specific Licences

12 <https://opensource.org/licenses/ISC>

Licence	Comments
Public Domain Dedication	Public domain dedication is not recognised in many jurisdictions, although it may take effect as a broad licence. CC-0 (see above) seeks to remedy this by providing an explicit fallback licence
Creative Commons NC variants	Non-commercial licences contain a restriction against a field of endeavour (commerce) contrary to paragraph 8 of the OSHWA criteria
Open Compute Project Licences (passive and copyleft)	Designed for hardware for use in OCP-compatible databases. The licences only really work when the various participants are patent holders, and are better regarded as standards-coupled licences

Table 4: Licences which are not compliant with OSHWA/ODI criteria

Note that both the Solderpad licence and the CERN OHL are in the process of revision. Version 2 of the Solderpad licence remains very similar to the Apache licence it is based on, but has been amended so that is now expressed to be a 'wraparound' of the Apache licence, rather than expressed as a different license. The advantages are that it is much easier for a practitioner familiar with Apache 2.0 to immediately see what the differences are between Solderpad and Apache 2.0.

As of January 2019, the CERN OHL is in the process of being modified significantly to produce version 2. Under current proposals this will be published in three variants: a permissive version which has an Apache-like effect, and two reciprocal versions – lesser and strong (strong reciprocal being the default for those who have already published hardware designs under current versions of the CERN-OHL with the ability to select a later version). Care has been taken to consult with developers of FPGAs and ASICs to try to meet their concerns, particularly around the use of proprietary tools and libraries that are all but unavoidable in practice, while retaining the copyleft nature of the reciprocal versions of the licence.

Desktop Analysis of Licence Adoption

The OSHWA Surveys

Across open hardware as a whole probably the most in-depth survey of open source hardware use and attitudes was undertaken by the OSHWA in 2012[13] and 2013.[14] This contained a small section on licence adoption. It should be noted that this survey covered open hardware in general, from mechanical items through to electronics, but there is no indication that any of those responding were involved in development at sub-component (i.e. chip design) level. Therefore, the results are both fairly out of date and of dubious relevance to chip design. One section of the survey related to licence adoption, and like the annual Black Duck licence adoption survey[15] counts all projects of equal weight. For example, in the Black Duck survey the Linux Kernel counts as a project with equal weighting to a tiny driver project which appears on GitHub but has never been used in commercial deployment). The results are therefore a dubious reflection of reality though it is interesting to note that very nearly 50% of the respondents had released projects with no explicit licence. It is difficult to interpret the results, as each respondent was permitted to respond with multiple answers to the

13 <https://www.oshwa.org/oshw-community-survey-2012/>
14 <https://www.oshwa.org/oshw-community-survey-2013/>
15 <https://www.blackducksoftware.com/top-open-source-licenses>

question of which licence they had used, but the thrust for open hardware in general (covering everything from mechanical devices and casings through to circuit boards) is that there is rough equality of deployment of copyleft licences (e.g. Creative Commons Share-Alike, GPL) and permissive (e.g. MIT, BSD, Creative Commons attribution-only) licences.

GitHub Search

Many open hardware projects are hosted on GitHub. CERN carried out some basic research on how many projects have adopted the CERN OHL by carrying out a Google search for "site:github.com CERN-OHL" that as of March 2018 produced[16] 657 results. It is misleading to assume these are all projects. However, undertaking a random sample of 10 pages from the complete Google results shows that around 80% of the results **are** projects. It is not easy to tell if these are unique results, but if they are, it suggests that something over 500 CERN-OHL licensed projects exist on GitHub. By comparison, TAPR OHL only generates 39 results of which 15 appear to be projects.[17] Solderpad shows 434,[18] almost all of which appear to be legitimate projects. It should be noted that it is more difficult to use this sort of search to find hardware projects licensed under Apache, MIT or BSD for the simple reason that the search will generate, overwhelmingly, software projects.

The OpenPiton Survey[19]

As part of a 2016 paper, Mohammead Shahrad, a member of the Princeton OpenPiton team, researched active processor core projects.[20] We have updated, corrected and verified the information presented and a summary in the table in appendix 2 under the section 'OpenPiton'.[21]

Of particular interest is that, when the projects are listed in order of the date of last active contribution, it is clear that the more recent projects are more heavily weighted towards permissive, rather than copyleft licensing. There is a total of 28 processor core products listed. There is a gap between October 2015 and February 2017, and if we take the projects that have been active since February 2017 (of which there are 15), 5 of them are copyleft. For projects prior to this date (of which there are 13), 12 are copyleft.

To summarise: recently active projects are split 33% copyleft, 67% permissive, as against the non-active projects, which are 92% copyleft, 8% permissive. This indicates a clear shift to permissive licensing for currently active projects.

16 As of 29 January 2019, this has increased to 'about 1500', but the search results are somewhat noisier, so it's not clear if this is a valid comparison.

17 We tried to rerun the search on 29 January, but the results were so much noisier that it's impossible to make a valid comparison.

18 We tried to rerun the search on 29 January, but the results were so much noisier that it's impossible to make a valid comparison.

19 Balkind, Joseph, et al. (2016) 'OpenPiton: An Open Source Manycore Research Framework', ASPLOS '16, pp 217 – 232. <http://parallel.princeton.edu/papers/openpiton-asplos16.pdf> DOI: 10.1145/2872362.2872414

20 <http://parallel.princeton.edu/openpiton/open_source_processors.php>

21 The results in the appendix have been updated to 29 January 2019, and therefore differ slightly from the version of the table provided to WD in the original version of the report. The figures above have been updated accordingly. For comparison, the text in the original report read: "There is a gap between October 2015 and February 2017, and if we take the projects that have been active since February 2017 (of which there are 12), 5 of them are copyleft. For projects prior to this date (of which there are 14), 12 are copyleft."

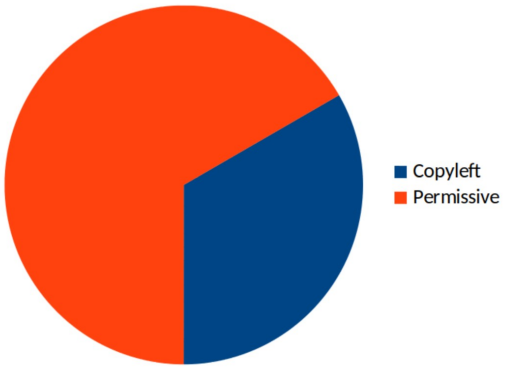


Fig. 1: Summary of licences chosen for recently active projects, data from the OpenPiton Survey

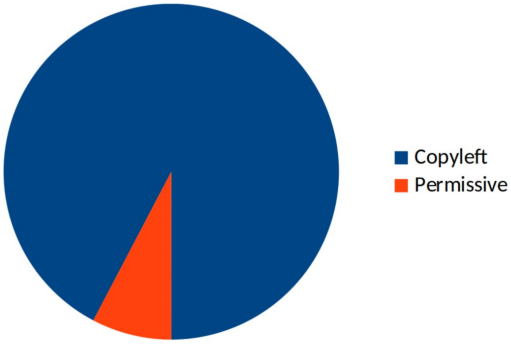


Fig. 2: Summary of licences chosen for non-active projects, data from the OpenPiton Survey

OpenCores and LibreCores

Two websites, opencores.org and librecores.org, host core designs and related materials such as tools and interfaces ('interfaces' are materials for other components which would typically appear on silicon alongside a core, such as UARTs and memory controllers). Opencores is run by a commercial entity, a situation which led to dissatisfaction from members of the FOSSi foundation regarding how Opencores operated, and their subsequent creation of Librecores as an alternative. Librecores has fewer projects, but they tend to be more active than Opencores (possibly because they have had less time to become obsolete).

There is a total of 1190 entries on the Opencores website, including software, toolchains, utilities and interfaces, as well as cores, of which 30 are marked verified. The Librecores site contains 90 entries but does not have any form of verification mechanism. We examined 24 entries in the Opencores website which are marked as 'verified' and 40 entries on Librecores. We selected entries which most

clearly relate directly to cores and interfaces, details of which are contained in appendices 3 and 4. There is also a thriving ecosystem of associated software tools, test suites and build and utility scripts, analysis of which is outside the scope of this report. Whilst we have undertaken a statistical analysis of this data, it is important to note that should be interpreted in the light of the following constraints:

(1) there is no easy way to weight each entry in terms of how pervasive and active the project is, so a barely-functional and rarely-adopted project would rank the same as a more mature and active one;

(2) there are significant projects which are not represented on either database;

(3) the selection of entries is largely subjective, and whilst the intention is to select projects which instantiate hardware (as opposed to toolchain or utility components), the selection was undertaken by a lawyer and not a microelectronics engineer, so mistakes are inevitable.

Various analyses of the licensing in both Opencores and Librecores for various categories of project are set out on Appendices 3 and 4.

Outcomes of the telephone interviews

Licensing – copyleft vs. permissive

All but one interviewee noted that a permissive model was the most likely to succeed from a commercial perspective. All acknowledged that a particular issue with copyleft licensing was that existing licences, including GPL and LGPL, and even CERN OHL did not provide sufficient certainty as regards boundaries delineating where the copyleft effect occurs. For example, if a component whose design is released under LGPL is combined with another component on the same silicon, does that mean that both components then have to be released under the LGPL? How about if the components are on separate chips? One interviewee specifically referred to the little-understood requirement in LGPL for sufficient interface information to be made available (together with the right to reverse engineer), for the LGPL component to be modified and re-linked to the 'work' as a whole. It is not clear how that would work with electronics especially since the works could be combined on static silicon (as masks). One interviewee noted that OpenSPARC (which was licensed under GPLv2) had in the past proved to a successful design (used for devices as diverse as digital cameras and network interfaces), thus demonstrating that GPL-based designs are capable of being commercially successful. There is little publicly available information on OpenSPARC (which is a relatively old project, having been released in 2006), and the interviewee suggested that separate research should be undertaken by locating some of the individuals who had been involved in the project initially, and in particular, the decision to open the technology, and to interview them.

Horizontal and Vertical Boundaries

Another interviewee made the explicit distinction between 'horizontal' boundary problems (as mentioned above), and 'vertical' boundary problems where it is not clear whether a requirement to release design documentation for a circuit design (or similar) also requires releasing the designs of the components themselves. It was noted that the CERN OHL explicitly deals with this via the requirement to release information for modifications at a similar 'level of abstraction' to the original design.[22] The current version of CERN OHL does not deal with the horizontal boundary problem

22 At of January 2019, proposals for CERN OHL v2 take a different approach and have introduced the concept of an 'Available Component'. Designs do not have to provide the design documentation for components that qualify as 'Available Components', which include items like readily available electronic components, provided that enough information about their specification, characteristics and interfaces is available to enable them to be sourced or used in the design. Thus a 555 timer when provided along with its datasheet would quality as an 'Available Component'.

(although this is to be addressed in the upcoming version 2 as mentioned above). The Open Hardware Description Licence (based on Mozilla Public License 2.0) does address this problem but is not frequently used.

One interviewee suggested the horizontal boundary problem might be fixed by saying that a weak copyleft licence could be drafted in a manner that the licensor provided an interface definition alongside the code. Provided that any third party complied with the interface definition, their code linking to the original licensor's code would be free of the reciprocal effect. The next version of the CERN OHL – see above – is likely to adopt an optional mechanism similar to this.

What drives licence choice (copyleft vs. permissive)?

Most interviewees expressed a preference for permissive licensing on the basis that existing copyleft licences left too much uncertainty, and that this uncertainty would inhibit adoption. It would also make it more difficult to deal with companies which provide proprietary libraries as those companies would be uncomfortable having their proprietary library used in a design which covered by copyleft of uncertain scope. One interviewee noted the value in copyleft licensing and noted that the Open Hardware Description licence expressly addressed the scope problems, but that it had not been widely adopted.

When it was suggested in each case that the next version of the CERN OHL would likely incorporate additional optional exceptions which expressly limited the reciprocal effect (as noted above) respondents suggested that this would cause them to potentially reconsider their licensing choices and consider its adoption. However, that there was little point in examining the issue in greater depth until such a licence was more widely accepted in the wild.

It was generally accepted that licence choice was ideological, and that some projects would be more inclined to wish to maximise use of their designs by providing them under a permissive licence while accepting the danger that the designs may become incorporated into proprietary hardware, while others wished to maximise freedom by making them available under a copyleft licence which ensured modifications would be made available under the same licence. However, all parties were all uncomfortable with existing copyleft licences, and regarded the issue, as this stage, as being largely hypothetical.

One interviewee noted that the use of components under copyleft licences in their current state would potentially cause difficulties with fundraising. One interviewee noted that in a due diligence exercise it was not unusual to run a code-scanning tool such as Black Duck against HDL files, although it is not immediately clear what the benefits of such an activity would be and whether Black Duck holds any HDL in its codebase, other than potentially to scan the code for licence texts such as the GPL which are frequently regarded as 'risky' by funders.

'Selling exceptions to the GPL'

One interviewee did note that it was possible that a design could be licensed under a restrictive copyleft licence of uncertain scope with respect to hardware such as the GPLv2 with a view to the licensor making a parallel proprietary licence providing certainty available for a fee. Clearly, this model tends to cause the licensor to use more restrictive licences in an effort to drive adoptees to the proprietary licence, whilst still permitting the licensor to describe the designs as 'Open Source [hardware]'. Richard Stallman, founder of the Free Software Foundation, has described this practice disparagingly as 'selling exceptions to the GPL'.[23]

23 Stallman, Richard 'Selling Exceptions to the GNU GPL' <https://www.gnu.org/philosophy/selling-exceptions.en.html>

One interviewee provided, as an example, the Leon core provided by Gaisler and based on SuperSPARC that is available both under LGPL/GPL and a proprietary licence. This was simply an illustration of dual licensing and does not suggest any particular motivation on the part of Gaisler for choosing that licensing model.

Open Hardware Communities

The consensus among interviewees was that the lack of open source or low-cost toolchains was an inhibiting factor in the growth of open hardware communities focusing on cores.

It is noteworthy that cores which emulate obsolete or obsolescent designs, primarily of interest to hobbyists, are more likely to be licensed under copyleft licences. For example, the Neo430, OpenMSP430 and T400 and T48 μController cores, examples of cores from selected OpenCores projects which fall into this category, are all licensed under copyleft licences.

After the initial phase of interviews, a second set of questions were sent to the interviewees focusing specifically on community building. We received two comprehensive responses within the time available, and both noted that permissive licences would be more attractive to commercial projects owing to avoidance of the problems around perceived linking. Both also pointed out that there probably was not enough data available to determine whether projects using non-open-hardware licences would have chosen an open hardware-specific licence if one was available. A potential illustration of this is that the OpenPiton list only three projects out of 26 chose a hardware specific licence (in all cases, the Solderpad licence.[24] In no case was a hardware-specific copyleft licence chosen.

Both responses also indicated that, most commonly, projects based on a permissive licence retained the same licence when out- bound licensing (i.e. the licence under which the design is to be licensed to third parties), as for the in-bound contributions.

In terms of community development, interviewees stressed the importance of evangelism and outreach, and funding community development. One individual also stressed the importance of becoming involved in projects like the FOSSi foundation.

Toolchains

One issue that came up frequently, although detailed discussion is outside the scope of this report, was that open source toolchains are much scarcer in the world of open hardware than they are in software. The extent to which the toolchain will incorporate code of its own into the output, and what the effect of that code is from a legal point of view, is highly problematic: it is a debatable point as regards software but becomes even more so when applied to hardware. Questions arise such as whether a bitstream is in any sense a computer program, and - if so - who 'runs' it when the hardware starts up.

Patents

The interviewees generally noted that patents were a potential problem but had no clear suggestions on how to address this challenge. It was noted that members of the RISC-V foundation get the benefit of a cross-licence agreement from the other members, but that non-members, although they are able to use the ISA specification freely, gain no form of explicit patent licence or protection.

24 The results in the appendix have been updated to 29 January 2019, and are not the version of the table provided to WD. The text of the version of the report released to WD accordingly read "two projects out of 26" in the sentence to which this is a footnote.

One interviewee noted that there was a move towards licences such as Apache 2.0 away from BSD or MIT because of its explicit patent provisions. One noted that the Solderpad licence (an Apache variant) had been adopted by LowRISC and PULPino because it was a relatively simple licence which had been modified specifically for hardware and had Apache-like patent provisions.

Establishing a default licence to use - recommendations

Broadly, licence choice should be limited to one of the more popular licences. Which specific licence is chosen depends depending on business needs for that the relevant project. The most popular software licence choices include the licences of the GPL family, Apache 2.0 and potentially MPL. For hardware, these may roughly correlate with CERN OHL/TAPR, Solderpad or BSD/MIT and Open Hardware Description License. Less well-used licences should be avoided, because they may cause licence incompatibility problems, and it makes project adoption more problematic. It is worth bearing in mind that the lawyers acting for counterparties prefer to work with the text of better-known licences to avoid having to spend expensive time to become familiarised with them. The informal drive towards licence standardisation is a topic which arises at legal licensing conferences quite frequently: the observation goes that the GPL, for all its flaws, is well understood, so tends to lead to a better legal outcome for both parties in contrast to a licence like (for example) the Open Software Licence, which is arguably better drafted, but less well used and understood.

It may be the case that there is, in practice, no choice that can be made, if the project uses, for example, a GPL component at its core which cannot be sufficiently decoupled from the rest of the work. In that case, the whole project would likely have to be released under the relevant version of the GPL.

For projects where there is no such constraint the specific choice of licence will depend upon the criteria of the specific project. The key question is whether the licensor is seeking to maximise either *utilisation* or *freedom*.[25]

If the licensor is seeking to maximise utilisation then a permissive licence such as Solderpad[26] will be most appropriate. In this case, the licensor must be comfortable that the software or hardware design may be incorporated into proprietary systems, and that the source code/design of any modifications may not be made available.

On the other hand, to maximise freedom, a good choice is the CERN OHL (adopting, where appropriate, one of the reciprocal versions, when v2 is released).

Another option as referred to previously in this paper is to sell proprietary unrestricted licences alongside a given open source licence (assuming the licences of the other components allow this). It is common practice to use a restricted licence (such as GPL or CERN OHL with no exceptions) to enhance the attractiveness of the proprietary option, though while this is common it is frowned upon by the GPL community. On the other hand, a legitimate reason for dual licensing may be that the licensee wishes to use a GPL-licensed core alongside third-party proprietary components, and therefore has to seek a licence from the licensor of the core which is compatible with those components.

25 In the sense of 'liberty'. In other words, the designer's intention is that the design, in all its incarnations, remains free of constraints on reuse, modification and distribution, and also has the effect of causing other designs combined with it to be equally free, with the overall intention of increasing the commons of free designs.

26 Or the newly (January 2019) announced permissive version of the CERN OHL.

Conclusion

All interviewees believed that the most commercially effective open hardware core designs were those which adopted permissive licences. The prevalence of these licences is borne out by desktop research. The stated various reasons for this are:

- that the currently available copyleft open hardware licences are insufficiently clear in their effect to be safely used;
- that the potential benefits of copyleft licensing in core designs are not yet sufficiently clear to show an overwhelming need to shift to a copyleft model;
- that copyleft licensing is certainly interesting and may have a place as the market matures. No interviewee was against copyleft core licensing in principle (although there was consensus that a weak copyleft with clearly defined boundaries was more likely to be commercially successful).[27]

Note that even though the interviewees selected were intended to represent a cross section of the core-developing communities, RISC-V was referred to by every interviewee. The emphasis on permissive licensing may therefore be an artefact of the relatively small sample size and a shared familiarity by the interviewees with RISC-V. It may, on the other hand, reflect a reality that RISC-V is the most prominent and widely adopted open ISA currently in use.

About the author

Andrew Katz *is a partner at boutique law firm Moorcrofts LLP, based in England's Thames Valley. Andrew specialises in technology law and has a particular interest in open design and development. He can be contacted at andrew.katz@moorcrofts.com*

27 At the time of the original research, some of the interviewees were aware that CERN was in the process of redrafting the CERN OHL to create a new version intended to address the concerns of FPGA and ASIC developers. The approach which was being taken at that stage was by way of application-specific exceptions to the licence. The current approach (as at January 2019) is somewhat different and now allows code libraries, macros, etc. which are provided as part of the toolchain to be included as an 'Available Component' - see footnote 22.

Appendix 1

Interviewees

- Krste Asanovic, Dept EECS, UC Berkeley.
- Andrew Back, Managing Director, AB Open.
- Julius Baxter, Director, FOSSi Foundation.
- Dr Jeremy Bennett, Chief Executive, Embecosm.
- Alex Bradbury, lowRISC CIC.
- David May, Professor of Computer Science, Bristol, Founder XMOS, FREng, FRS.
- Simon Phipps, Founder, Meshed Insights Ltd.
- Dr Davide Rossi, University of Bologna.

Appendix 2

Taxonomy of Open Source Processors from OpenPiton

Processor	Architecture	Licence	Last Update to Project	Last Update to Code
aeMB	32b MicroBlaze	LGPL v3	Feb 2012	-
AltOr32	32b ORBIS	LGPL v3	Feb 2015	Jun 2014
Amber	32b ARM v2a	LGPL	Sept 2017	Nov 2015
Ariane	64b RISC-V	Solderpad	Jan 2019	-
BERI	64b MIPS/CHERI	BERI HW-SW	Mar 2017	-
CPU86	16b x86	GPL	Jun 2014	-
LatticeMicro32	32b LatticeMicro32	GPL	Oct 2017	-
LEON 3	32b SPARC v8	GPL	Dec 2017	-
MIAOW GPGPU	AMD Southern Islands	BSD 3-Clause & GPL v2	Sept 2017	-
MIPS32 r1	32b MIPS 32 rl	LGPL v3	Jul 2015	-
mor1kx	32b ORBIS	OHDL	Jan 2019	Jan 2019

Processor	Architecture	Licence	Last Update to Project	Last Update to Code
openMSP430	16bMSP430	BSD	May 2018	Apr 2018
OpenPiton	64b SPARC v9	BSD 3 Clause & MIT	Jan 2019	-
OpenRISC	32b/64b ORBIS	LGPL	Nov 2018	-
OpenScale	32b MicroBlaze	GPL v3	Jan 2012	-
OpenSPARC T1/ T2	64b SPARC v9	GPL v2	Nov 2008	-
or1200	32b ORBIS	LGPL	Oct 2015	Jun 2015
pAVR	8b AVR	GPL v2	Jul 2009	Mar 2009
Pico RV	32b RISC-V	ISC	Nov 2018	Nov 2018
PULP-RI5CY	32b RISC-V	Solderpad	Jan 2019	-
RISC-V Boom	64b scalar RISC-V	BSD 3-clause	Jan 2019	-
RISC-V Rocket	64b scalar RISC-V	BSD 3-clause	Jan 2019	-
SecretBlaze	32b MicroBlaze	GPL v3	Dec 2012	Dec 2012
Simply RISC S1	64b SPARC V9	GPL v2	Dec 2008	-
XUM	32b MIPS32 r2	LGPL v3	Jul 2015	-
Zeroriscy	32b RISC-V	Solderpad	Nov 2018	-
Zet	16b x86	GPL v3	Nov 2013	-
ZPU	32b MIPS	FreeBSD + GPL	Apr 2015	-

Table 5: Taxonomy of differences of open source processors (table data last checked 29 January 2019). [28]

28 Originally published in Balkind, Joseph, et al. (2016) 'OpenPiton: An Open Source Manycore Research Framework', ASPLOS '16, pp 217 – 232. <http://parallel.princeton.edu/papers/openpiton-asplos16.pdf> DOI: 10.1145/2872362.2872414, Table 4, updated at http://parallel.princeton.edu/openpiton/open_source_processors.php

Appendix 3

OpenCores

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
Elliptic Curve Group (ecg)	OpenCores	The Elliptic Curve Group core is for computing the addition of two elements in the elliptic curve group, and the addition of c identical elements in the elliptic curve group and it is carefully optimized for FPGA	LGPL	Component	Copyleft
Reed Solomon Decoder (204,188)	OpenCores	Reed Solomon Decoder (204,188), with T=8	GPL	Component	Copyleft
Viterbi Decoder (AXI4-Stream compliant)	OpenCores	A fully configurable VHDL Viterbi decoder compliant with the AXI4-Stream interface	GPL	Component	Copyleft
Ethernet 10GE MAC (xge_mac)	OpenCores - GitHub	The 10GE MAC Core implements the Media Access Control functions for 10Gbps operation as defined in IEEE Std 802.3ae.	LGPL	Interface	Copyleft
Ethernet MAC 10/100 Mbps (ethmac)	OpenCores	The Ethernet MAC (Media Access Control), sublevel within the Data Link Layer of the OSI reference model. This core is designed for implementation of CSMA/CD LAN in accordance with the IEEE 802.3 standards.	LGPL	Interface	Copyleft
sd card controller (sdcard_mass_storage_controller)	OpenCores	The "sd card controller" is a Secure Digital Card Host Controller, which main focus is to provide fast and simple interface to SD/SDHC cards.	LGPL	Interface	Copyleft

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
Small 1-wire (onewire) master, with Altera tools integration (sockit_owm)	OpenCores	This IP implements the 1-wire communication protocol (http://en.wikipedia.org/wiki/1-Wire).	LGPL	Interface	Copyleft
PCIe SG DMA controller	OpenCores	This package involves a PCIe Scatter-Gather DMA engine for Virtex5 and Virtex6 and implements MAC, Physical (Xilinx Hard and Soft IP Cores) and Transaction Layer (Custom Core) of PCIe.	LGPL	Interface	Copyleft
Wupper: PCIe DMA Engine for Xilinx FPGAs (virtex7_pcie_dma)	OpenCores	A system controller primarily designed to provide an interface to standard FIFOs (a simple Direct Memory Access (DMA) interface to the Xilinx Virtex-7 PCIe Gen3 hard block.)	LGPL	Interface	Copyleft
8/16/32 bit SDRAM Controller (sdr_ctrl)	OpenCores - GitHub	8/16/32 Configurable SDRAM data width which is Wish Bone compatible.	GPL	Interface	Copyleft
High Performance Dynamic Memory Controller (hpdmc)	OpenCores	HPDMC is part of the Milkymist System-on-Chip, the most advanced open source SoC for interactive multimedia applications.	GPL	Interface	Copyleft
VGA/LCD Controller (vga_lcd)	OpenCores	The OpenCores VGA/LCD Controller core is a WISHBONE revB.3 compliant embedded VGA core capable of driving CRT and LCD displays. It supports user programmable resolutions and video timings, which are limited only by the available WISHBONE bandwidth.	GPL	Interface	Copyleft

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
I2C controller core (i2c)	OpenCores - GitHub	I2C is a two-wire, bidirectional serial bus that provides a simple, efficient method of data exchange between devices. It is primarily used in the consumer and telecom market sector.	BSD	Interface	Permissive
UART to Bus (uart2bus)	OpenCores	The UART to Bus IP Core is a simple command parser that can be used to access an internal bus via a UART interface and provides a quick and easy way to test a new FPGA board.	BSD	Interface	Permissive
Plasma - most MIPS I(TM) opcodes (plasma)	OpenCores	The Plasma CPU is a small synthesizable 32-bit RISC microprocessor currently running a live web server with an interrupt controller, UART, SRAM or DDR SDRAM controller, and Ethernet controller.	Others	Pcore	
Tate Bilinear Pairing	OpenCores	The Tate Bilinear Pairing core is specially designed for running Tate bilinear pairing algorithm for hyperelliptic curve $y^2=x^3-x+1$ defined over $GF(3^m)$, where $m=97$ and $GF(3^m)$ is defined by x^97+x^12+2 and it is carefully optimized for FPGA.	LGPL	Pcore	Copyleft
Amber ARM-compatible core (amber)	OpenCores	The Amber processor core is an ARM-compatible 32-bit RISC processor. The Amber core is fully compatible with the ARM® v2a instruction set architecture (ISA) and is therefore supported by the GNU toolset.	LGPL	Pcore	Copyleft
NEO430 Processor (MSP430-compatible)	OpenCores and librecores	This processor is based on the Texas Instruments MSP430 ISA and provides 100% compatibility with the original instruction set but is not an MSP430 clone.	LGPL	Pcore	Copyleft

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
minsoc	OpenCores	The Minimal OpenRISC System on Chip is a system on chip (SoC) implementation with standard IP cores available at OpenCores.	LGPL	Pcore	Copyleft
CORDIC core	OpenCores	The CORDIC algorithm is an iterative algorithm to evaluate many mathematical functions, such as trigonometrically functions, hyperbolic functions and planar rotations.	GPL	Pcore	Copyleft
T400 µController (t400)	OpenCores	The T400 µController is an implementation of National's 4-bit COP400 microcontroller family architecture intended to be used as a replacement for the original chip in SOCs recreating legacy systems.	GPL	Pcore	Copyleft
T48 µController	OpenCores	The T48 µController core is an implementation of the MCS-48 microcontroller family architecture. While being a controller core for SoC, it also aims for code-compatability and cycle-accuracy so that it can be used as a drop-in replacement for any MCS-48 controller.	GPL	Pcore	Copyleft
openMSP430	OpenCores - librecores	The openMSP430 is a synthesizable 16bit microcontroller core written in Verilog. It is compatible with Texas Instruments' MSP430 microcontroller family and can execute the code generated by any MSP430 toolchain in a near cycle accurate way.	BSD	pcore	Permissive

Table 6: OpenCores

Appendix 4

Librecores

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
ZAP ARM Processor	librecores	ZAP is a pipelined ARM processor core that can execute the ARMv4T instruction set. It is equipped with ARMv4 compatible split writeback caches and memory management capabilities.	GPL	pcore	Copyleft
mor1kx	librecores	This repository contains an OpenRISC 1000 compliant processor IP core.	MPL 2.0 RC2	pcore	Copyleft
neo430	librecores	This processor is based on the Texas Instruments MSP430 ISA and provides 100% compatibility with the original instruction set but is not an MSP430 clone	LGPL	pcore	Copyleft
kpu-soc	librecores	KPU is a minimal system on chip (SoC) created for use as a testbench for the KPU core	GPL	pcore	Copyleft
PULPino	librecores	Single-core microcontroller system based on 32-Bit RISC-V cores (ETH Zurich)	SOLDERPAD HW LICENCE V0.51	pcore	Permissive
parallella-riscv	librecores	Integration of the RISC-V rocket core, inside the Zynq FPGA device of Parallella	MIT and The Regents of the University of California	pcore	Permissive
RgGen	librecores	Code generation tool for control/status in a SoC design	MIT	pcore	Permissive
picorv32	librecores	PicoRV32 is a CPU core that implements the RISC-V RV32IMC Instruction Set. It can be configured as RV32E, RV32I, RV32IC, RV32IM, or RV32IMC core, and optionally contains a built-in interrupt controller.	ISC	pcore	Permissive

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
SimpleVOut	librecores	A simple set of FPGA cores for creating video signals in various formats.	ISC	pcore	Permissive
NyuziProcessor	librecores	Nyuzi is an experimental GPGPU processor hardware design focused on compute intensive tasks. It is optimized for use cases like deep learning and image processing.	Apache v2.0	pcore	Permissive
riscv-sodor	librecores	educational microarchitectures for risc-v isa	Sodor based on the BSD 3-clause licence	pcore	Permissive
TV80 Z80-compatible microprocessor	librecores	TV80 is a Z80-compatible synthesizable Verilog core and aims to be an area-efficient core which closely mimics the original operation and cycle timing of the Zilog Z80.	MIT	pcore	Permissive
Ariane	librecores	Ariane is a 6-stage, single issue, in-order CPU which implements the 64-bit RISC-V instruction set. It has configurable size, separate TLBs, a hardware PTW and branch-prediction (branch target buffer and branch history table). The primary design goal was on reducing critical path length.	Solderpad v0.51	pcore	Permissive
RV12 RISC-V Processor	librecores	The RV12 is a highly configurable single-issue, single-core RV32I, RV64I compliant RISC CPU intended for the embedded market.	other	pcore	
openGFX430	librecores	The openGFX430 is a synthesizable Graphic controller written in Verilog and tailored for the openMSP430 core.	3-Clause BSD	interface	Permissive

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
liteeth	librecores	LiteEth provides a small footprint and configurable Ethernet core whose aim is to lower entry level of complex FPGA cores used in today's SoC such as Ethernet, SATA, PCIe, SDRAM Controller.	2-clause BSD	interface	Permissive
litesata	librecores	LiteSATA provides a small footprint and configurable SATA gen1/2/3 core whose aim is to lower entry level of complex FPGA cores used in today's SoC such as Ethernet, SATA, PCIe, SDRAM Controller	2-clause BSD	interface	Permissive
litedram	librecores	LiteDRAM provides a small footprint and configurable DRAM core whose aim is to lower entry level of complex FPGA cores used in today's SoC such as Ethernet, SATA, PCIe, SDRAM Controller	2-clause BSD	interface	Permissive
litepcie	librecores	LitePCIe provides a small footprint and configurable PCIe gen1/2 core whose aim is to lower entry level of complex FPGA cores by providing used in today's SoC such as Ethernet, SATA, PCIe, SDRAM Controller	2-clause BSD	interface	Permissive
litejesd204b	librecores	LiteJESD204B provides a small footprint and configurable JESD204B core whose aim is to lower entry level of complex FPGA cores by providing used in today's SoC such as Ethernet, SATA, PCIe, SDRAM Controller	2-clause BSD	interface	Permissive
EurySpace	librecores	Space Communication System based on CCSDS recommendations	MIT	interface	Permissive

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
HDMI2USB	librecores	The HDMI2USB project develops affordable hardware options to record and stream HD videos (from HDMI & DisplayPort sources) for conferences, meetings and user groups.	2-clause BSD	interface	Permissive
USB 1.1 Device IP Core	librecores	USB 1.1 slave/device IP core derived from USB 2.0 Function IP core save that all the high speed support logic has been ripped out and the interface changed from shared memory to FIFO based	3-clause BSD	interface	Permissive
USB 2.0 Device IP Core	librecores	This is a USB 2.0 compliant core. Due to the high interface speed, an external PHY will be required and an industry standard PHY interface for USB has been developed. This interface is called USB Transceiver Macrocell Interface (UTMI) and is WISHBONE SoC compliant.	3-clause BSD	interface	Permissive
AES (Rijndael) IP Core	librecores	AES (Rijndael) IP Core (128 bit version)	3-clause BSD	interface	Permissive
NoC Implementation Written in SystemVerilog	librecores	This is a Network on Chip (NoC) Router/Fabric implementation written in SystemVerilog.	Apache v2.0	interface	Permissive
MIPI CSI-2 Receiver	librecores	This project is an open source (MIT license) MIPI CSI-2 receive core for Xilinx FPGAs, supporting 4k resolution at greater than 30fps.	MIT	interface	Permissive
Wishbone	librecores	Wishbone is an interconnect for Systems-on-Chip.	other	interface	
scct	librecores	SCCT is a Simple Capture/ Compare Timer written in Verilog. It provides multiple capture/compare channels that use a common counter.	GPL	component	Copyleft

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
libstorage	librecores	Library of RTL components for data storage	ISC	component	Permissive
The PicoBlaze-Library	librecores	The PicoBlaze-Library offers several PicoBlaze devices and code routines to extend a common PicoBlaze environment to a little System on a Chip (SoC or SoFPGA).	Apache v2.0	component	Permissive
PicoBlaze-Examples	librecores	PoC - "Pile of Cores" provides implementations for often required hardware functions such as FIFOs, RAM wrapper, and ALUs.	Apache v2.0	component	Permissive
The PoC-Library	librecores	PoC - "Pile of Cores" provides implementations for often required hardware functions such as Arithmetic Units, Caches, Clock-Domain-Crossing Circuits, FIFOs, RAM wrappers, and I/O Controllers.	Apache v2.0	component	Permissive
litescope	librecores	LiteScope is a small footprint and configurable embedded logic analyzer for use in an FPGA and aims to provide a free, portable and flexible alternative to large vendor solutions	2-clause BSD	component	Permissive
WISHBONE Interconnect IP Core	librecores	This is a WISHBONE Interconnect Matrix IP core.It can interconnect up to 8 Masters and 16 Slaves.	3-clause BSD	component	Permissive
sha256	librecores	Hardware implementation of the SHA-256 cryptographic hash function with support for both SHA-256 and SHA-224	2-clause BSD	component	Permissive

Name of Project	Where Project is Recorded	Brief Description	Type of Licence	Category	Licence Type
siphash	librecores	This is a hardware implementation of the SipHash [1] keyed hash function written in Verilog 2001 and is designed as a self contained core that performs the message block processing including initialization, compression and finalization operations.	2-clause BSD	component	Permissive

Table 7: LibreCores

Appendix 5

Analysis

		OpenCores	Librecores	Total
Type of project	Processor Core	9	14	**23**
	Component	3	9	**12**
	Interface	11	14	**25**
TOTAL:		**23**	**37**	**60**

Table 8: Summary Analysis

		OpenCores	Librecores	Total
Licences	Copyleft	19	5	**24**
	Permissive	3	30	**33**
	Other	1	2	**3**
Total:		**23**	**37**	**60**

Table 9: Licence Analysis

		Processor Core	Component	Interface	Total
OpenCores	Copyleft	7	3	9	**19**
	Permissive	1	0	2	**3**
	Other	1	0	0	**1**
Total:		**9**	**3**	**11**	**23**

Table 10: OpenCore Analysis

		Processor Core	Component	Interface	Total
Librecores	Copyleft	4	1	0	**5**
	Permissive	9	8	13	**30**
	Other	1	0	1	**2**
Total:		**14**	**9**	**14**	**37**

Table 11: Librecore Analysis

		Processor Core	Component	Interface	Total
	Copyleft	11	4	9	**24**

		Processor Core	Component	Interface	Total
Both	Permissive	10	8	15	**33**
	Other	2	0	1	**3**
Total:		**23**	**12**	**25**	**60**

Table 12: Analysis of Opencores and Librecores

Chapter 18

Determining the True Openness of Open Source Projects (Ibrahim Hadad)


DETERMINING THE
TRUE
OPENNESS
OF OPEN SOURCE PROJECTS
IBRAHIM HADDAD, PHD
THE LINUX FOUNDATION

Ibrahim Haddad, PhD

Determining the True Openness of Open Source Projects

The motivation for writing this paper originated from various discussions evolving around what makes a project a true open source project beyond just the choice of license. People have different opinions and thoughts about the various indicators of a project's openness. In this paper, we explore such indicators that together can help define the true openness of a given project and conclude with some recommended practices and other practices to avoid in an open source project, touching on a dozen different areas. We hope this paper becomes a trigger for new conversations in open source projects on how to be more open, transparent, and inclusive.

Printed in the United States of America

First Edition, 2019

1 Letterman Drive
Building D
Suite D4700
San Francisco CA 94129

Contents

Introduction

The success of an open source project depends on many factors, where openness is one of the essential ones. The primary premise of this paper is to explore and identify the various indicators that can provide insights about the openness of a given project. The paper is organized in four sections:

- **Openness indicators:** This section examines such indicators and discusses how they contribute to the openness of the overall project.
- **Best and worst practices:** This section provides recommendations for practices that can enable and foster an open environment that will help open source projects grow and prosper. The section also covers some of the worst practices that you want to absolutely avoid.
- **Characteristics of a great open source community:** This section offers thoughts on the common characteristics of successful and thriving open source project communities.
- **Call to action:** This section focuses on how participants in open source projects can do a better job with respect to openness.

Chapter 1

OPENNESS INDICATORS

GOVERNANCE

Governance determines who has influence and control over the project beyond what is legally required in the open source license. A project's governance model establishes a collaboration framework that addresses difficult questions such as:

Contributions

- Who makes decisions for code inclusion and releases, and how?
- Who can be the lead maintainer or architect for the project (larger projects have more than one)?
- How can the project contributors become maintainers or committers?

Direction and Finance

- How can the project raise money and who decides how this money is spent?
- Should the project have a Technical Steering Committee or a Conformance and Certification Committee? Who can be on them?
- Who decides the project's direction and roadmap?

Transparency

- Who can participate in the discussions and decide on critical matters?
- How transparent are the decision-making processes?
- Can anyone follow the discussions and meetings that take place in the project?

Re-use

- What compliance requirements are there for redistributing, modifying or using the software?
- How can the project enable contributors and downstream re-distributors to comply with these requirements?

Copyright and trademark

- Who owns the copyright on contributed code?
- How can users license the project's branding?

ACCESS

A key indication of project openness is how publicly accessible the project's resources, communications (mailing lists, IRC, Slack, etc.) and history are, beyond the current active participants. For starters, an open project will provide the same level of source code availability to all developers, meaning there is no favoritism to developers via priority access.

Collaboration in most open source communities is centered on a relatively standardized set of tools, such as wikis, IRC, and mailing lists, which allow members of the community to communicate with each other. It is worth noting though that there may be circumstances where mailing lists with limited distribution are appropriate, e.g. for handling pre-disclosure security vulnerability reports, however, these are rare and special cases. Open source communities often rely on tools such as GitHub, git, Bugzilla, JIRA, and file servers to collaborate on code development; wikis and blogs are often used to inform about the community efforts. Project policies and infrastructure must be in place to ensure developers can adequately interact with each other using these tools.

Additionally, open projects provide access to developer tools such as mailing lists, forums, bug-tracking systems, source code repositories, and documentation. Participants are able to join discussion platforms, decision-making mechanisms, and project roadmaps so it is possible to understand why and how the project makes decisions.

PROCESSES

A project with a high degree of openness will have clearly defined processes for how things work in the community and how to contribute to the project. For starters, a clear development process should outline how to incorporate code into the project, the release process and schedule of the project, and any requirements developers need to meet to get their code accepted. This should also include guidelines for participation that demonstrate community best practices for things like patch submissions, feature requests, bug reports, and signing-off on code contributions.

DEVELOPMENT

An open development process enables developers to influence the direction of the project via contributions. It encourages contributions through the visible recognition of the developers and the provision of a transparent contribution and acceptance process that provides clear feedback on updates to contributions as they are incorporated into the project. This transparency should also allow external participants to identify the source from which code contributions originated.

Release early and release often is a practice that has been integral to open source software for most of its history. This practice allows open source communities to innovate at a rapid pace with a high quality of code because it creates a much faster feedback loop between developers, testers, and users. Releasing early allows feedback at an earlier stage of development so new ideas can be incorporated while the code is still flexible; it also allows any potential issues to be flagged more quickly. Releasing often results in smaller changes that are easier to understand, debug, and improve which makes it much easier to maintain a rapid development pace. This practice also aligns well with the progressive movement of many industry projects towards agile development and continuous integration / continuous delivery (CI/CD) methodologies.

COMMUNITY STRUCTURE

Open source project communities usually start with a flat structure and transition to a hierarchical structure as they grow in terms of contributors, and as the body of code becomes more complex, requiring additional maintainers. From that perspective, the code leadership evolves around committers, maintainers, and reviewers (please note that not all projects support these levels of contributors).

Two key factors that indicate the openness of a project's community structure are:

1. The commitment that individuals responsible for the project leadership get their roles based on talent, effort, and achievements in the project.
2. A key component of community openness is the accessibility to become a committer, reviewer, or maintainer. This process should be clearly documented and equitable so that any contributors to projects have the potential to be promoted to one of these roles.

RELEASE NOTES

In open source projects, with hundreds and possibly thousands of developers, documenting releases is a fundamental requirement. There are many advantages that result from providing detailed release notes, such as providing visibility into the project's progress, documenting continuous improvements to the project with every release, providing a great reference for new users of developers joining the project, and in general using it as a communication tool.

Another possible related openness indicator is how the project offers credit to all contributors via the release notes or a specific file that lists all contributors.

ROADMAP

At a high level, roadmaps provide high-level overviews of the project's goals and deliverables for that release. Open source projects that maintain an open roadmap achieve several advantages and are able to:

- Communicate the plans and goals for each release (minor, major, etc.),
- Manage the expectations of its users and developers by generating a shared understanding across everyone involved in the project, and
- Expose the project's plans to other open source projects that possibly rely upon or use them as a dependency.

LICENSE AND INTELLECTUAL PROPERTY CONSIDERATIONS

License

The license of an open source project determines the rights to use, copy, modify, and distribute the code. The choice of license for an open source project is an essential factor in determining the openness of the project. Open source projects should only use licenses that are approved by the **Open Source Initiative** and/or recognized as "free / libre" by the Free Software Foundation. Such licenses allow software to be freely used, modified, and shared. To be approved by the Open Source Initiative, a license must go through their l**icense review process** to confirm that the license satisfies their **Open Source Definition** ("OSD"). You may come across many other licenses that are incompatible with the OSD. Most of these licenses are considered "Source Available" licenses that commonly include restrictions or limitations on the use and/or distribution of the software. These restrictions often render the licenses as incompatible with the OSD.

Derivatives

Developers should be able to create and distribute derivatives of the source code for their own projects or reuse the code in other projects. To allow this, the project needs to be available under an appropriate license that provides these freedoms.

Contribution mechanisms

A key consideration for any project is the mechanism by which they manage the provenance of incoming code contributions. Open source projects deal with these concerns differently. Some projects adopted a developer certificate of origin, others require a contributor license agreement, while many projects (particularly smaller ones) do not use formal contribution provenance mechanisms.

DCO sign-off process

The Developer Certificate of Origin (DCO) sign-off process ensures that every single line of code accepted into a project has a clear audit trail. It is a developer's certification that they have the right to submit code for inclusion into the project. The Linux kernel process for instance requires all contributors to sign-off their code, which indicates the contributor certifies the code as outlined in the **Developer Certificate of Origin**. The signature communicates that the contributor has created or received the contribution under an appropriate open source license that allows it to be incorporated into the project's code base under the license indicated in the file. The DCO establishes a chain of people who take responsibility for the licensing and provenance of contributions to the project.

Contributor license agreement (CLA)

Some projects require either developers or their employers signing a CLA. Unlike the DCO, the text of CLAs can vary significantly from project to project, so the terms of any given CLA may have different effects. The purpose of a CLA is to ensure that the guardian of a project's outputs has the necessary ownership or grants of rights over all contributions to allow them to distribute under the chosen license. In some cases, this even means that the contributor will grant an irrevocable license, which allows the project to distribute the contribution as part of the project.

Software Package Data Exchange license format

Many of these open source projects have code licensed under different

licenses. Some projects are already adopting the **SPDX** format as a method to communicate the license information. One openness indicator could be how well a project makes explicit the various licenses for its different pieces of code via the standardized SPDX short-form license identifiers in every file. Additionally, a project can provide detailed license, copyright and other related information in a standardized, open, human-readable and machine-readable format by providing a bill of materials as an SPDX document.

DOCUMENTATION

An open source project can provide different types of documentation to help both users and developers of its community. Historically, documentation has been an area that is lacking and requires improvements. However, this is changing and many of the projects, especially those hosted within an open source foundation, have great documentation that cover all areas of the projects. In the following subsections, we examine three core areas where documentation is essential.

- Project
    - Mission
    - Governance
    - Community structure
    - Release cadence
    - Roadmap and priorities
    - Use cases
    - FAQs
- Documentation targeted for users:
    - User guide and tutorials
    - API guide
    - Architecture overview
    - Installation guide
    - Feature request process
    - Experience sharing section
- Documentation targeted for developers:
    - Detailed architecture and mapping to code sub-systems/ services when applicable

- Development process
- How to get involved
- Guidelines for participation
- Feature request process
- Patch submission process
- Signed-off-by process, when applicable
- Developer guides and tutorials
- API guide

Chapter 2

RECOMMENDED BEST PRACTICES

In this chapter, we highlight some of the recommended practices that support and enable open source projects, and also provide some practices to avoid.

	Recommended Practices	Practices to Avoid
License	OSI-approved open source license or FSF free/libre license.	• No license. • Unclear or conflicting licensing terms. • Vanity license. • Create a new license.
Governance	A governance model that gives equal footing to all current and future contributors to the project. Open source projects with an open and transparent governance model have better chances to grow, have a healthy environment, and attract developers and adoptees.	• No governance. • Biased governance that is dominated by a given party, usually the founder of the project.
Access	• Project resources are accessible to any users or developers interested in the project. • Anyone can participate in the project. • Any participant can earn committer rights by way of contribution and build trust with the project's community.	• Limited access based on sponsorship level or other factors.
Processes	• Documented processes for requesting a feature, reporting bugs, submitting code, etc. • Code is only committed through the project's defined process for incoming contributions. • All code goes through a peer review process.	• Ad-hoc or poorly designed processes. • Processes that keep changing or are stale and need improvements in order to scale and accommodate the development status of the project. • Processes that are not followed or respected.

	Recommended Practices	Practices to Avoid
Processes (Continued)	• The process to become a committer / maintainer / reviewer is enforced by the project for consistency. • The project's community revises its processes based on incoming feedback to ensure they continue to meet the project's needs as it grows and scales.	
Development	• Responsibility for development allocated to the individuals with the best capacity to deliver. • The project enforces quality standards when merging code. • The project implements multiple levels of review before entering final release. • Peer review is mandatory and public.	• Peer review is not enforced. • Pedigree of incoming code is not verified. • Project does not have a sign-off process or equivalent. • Contributors do not follow sign-off process while the code is still merged.
Community	• Accessible to newcomers - open development generally strives for inclusiveness. • Focused on visibility with emphasis on open decision-making processes and communication. • Self-organizing where individuals contribute in their areas of interest, or those of their employers. • Resilient to organizational change given that leadership is earned with experience. If individuals cease to participate, there are others to take their place.	• Little or no help or support available to new developers entering the project in terms of guidance, documentation, and mentorship. • Obscure decision-making process.
Community Structure	• Meritocracy drives advancement and acceptance. Contributors who provide the most value to the community are granted project leadership roles. • The project welcomes newcomers who have freedom and access to participate in public discussions, development, and testing.	• Structure biased towards a certain company, coalition, or commercial interests. • No clear path for developers on how to be promoted to a committer, reviewer, or maintainer.

	Recommended Practices	Practices to Avoid
Community Structure (Continued)	• The project's hierarchy is scalable because it consists of maintainers who oversee specific bodies of code in levels that can be added or removed as needed based on the size of the community. • Anyone can submit patches, and both developers and users are involved in the testing process. The roles of developer and user are closely integrated in open source development, allowing users to have a more direct path to influencing the project.	
Releases	• To protect certain users from the instability of rapidly developing software, projects provide stable releases that restrict the addition of experimental features to provide a reliable version that better supports use cases that rely on stability. • Weekly or monthly stable releases provide users and developers with the newest functionality after it has been tested • Long-term stable versions extend to longer periods and often only include security patches and bug fixes.	• Unclear structure of releases and branches. • Undocumented release processes. • Documented processes but uncommunicated and/or hard to locate on the wiki or the web site of the project.
Release Cadence	• The project has a defined cadence for its releases with set goals per release. • The release cadence and the goals to be met by each release are known to all projects stakeholders.	• No release cadence • Cadence is not suitable or does not meet the needs of the end users.
Derivatives	Open source license provides the freedom to create and distribute derivatives.	Non-OSI approved license or non FSF free/libre license that limits these freedoms.
Communication tools	Such tools include mailing lists and IRC, among others, and are available and open to anyone wishing to participate in the project.	• Restricted access to some of the communication tools. • Discussions happening in private chat rooms or private mailing lists.

	Recommended Practices	Practices to Avoid
Transparency	Open source communities must be as transparent as possible to attract new participation. • Contribution transparency. • Peer review transparency. • Transparency of discussions. • Transparency of promotion to committer or maintainer.	• Ambiguous decision-making process. • Favoritism in code acceptance based on origin and not quality of code and result of peer review. • Discussions with direct impact on project (architecture, development) happen in private with some rare exceptions of communication that for instance relate to the distribution of pre-disclosure security vulnerabilities.
Development tools	Available and open to all.	• Limited access. • Dependencies on proprietary tools prohibiting non-corporate contributors from participating in the development efforts.
Documentation	Availability of documentation covering architecture, APIs, installation guides, developer guides, development processes, participation guides, tutorials, etc.	• No documentation (source code is documentation) • Poor documentation. • Unmaintained documentation.

Chapter 3

CHARACTERISTICS OF A GREAT OPEN SOURCE COMMUNITY

Great open source communities may differ in what they work on and how they implement the structure and processes of their projects, but they share several characteristics:

- Community members work together for a common goal with a high sense of cooperation.
- Project participants feel free to express their opinions, share their ideas, and engage with other project members.
- Community members chose their maintainers and committers based on their expertise, level of contributions, and thought leadership. The community maintains a clear process for the selection criteria.
- The project's community is accessible to newcomers as users of the project or developers who wish to participate and contribute. Open development strives for inclusiveness.
- Great open source communities are very transparent with a strong emphasis on open decision-making processes and communication.
- Great open source communities are resilient to organizational change. Leadership is earned with experience and with the approval and consensus from community members. If individuals cease to participate in the project, there are others to take their role with minimal disruptions to the project and a clear process to guide the selection of the new leaders (maintainers).
- Great open source communities work to ensure that those who fall in minority populations are not treated differently. These communities give a voice to minority populations through frequent

consultation with members of those societies about how the community can improve to meet their needs better.

- Great communities do not limit contributions to just code and offer a wide range of contribution opportunities for non-coders in areas such as testing, documentation, communication, marketing efforts, and many more.
- Great open source communities foster a feeling of connection and collaboration among its members by providing plenty of opportunities for interaction. They create a feeling of connection that makes members more motivated to work towards the projects' goals.

A healthy and strong open source community is inclusive and diverse. Many open source projects are working to increase their inclusiveness, the diversity of their contributors, and to encourage new participation.

Chapter 4

CALL TO ACTION

This chapter focuses on the question of how we can do a better job with respect to openness. Three primary players come to mind:

- Open source developers – create new open source projects, contribute to existing projects.
- Open source leadership – on behalf of their company, they encourage and support the participation of internal engineers to open source collaborative projects; they support stakeholders and compliance teams in decisions to open source internal code; they foster discussion with their peers at other companies; they investigate opportunities to create new open source projects and collaborations.
- Open source foundations – such foundations host open source projects within a neutral forum, create new open source projects in support of their members, mentor developers, advise projects on policy issues, etc.

We believe these three key roles are instrumental in shaping the openness on any open source project. In the following table, we identify some of the actions these players can exert in the various areas that would help an open source project get to a higher level of openness.

	Open Source Developer	Open source Leadership	Open Source Foundation
License	• Avoid projects with vanity or unclear licenses. • Choose an OSI-approved license for their own project(s). • Communicate the benefits of using an OSI-approved open source license to colleagues. • Understand the license choice of your project or the license of the project(s) you want to participate in.	• Open source code using OSI-approved licenses only. • Mentor company executive on the adoption hurdles a vanity license poses.	• Educate hosted projects on the right choice of license for their projects. • Support selection of an OSI-approved license. • Provide the ability for companies to collaborate on projects in a neutral environment. • Act as an agent for the project, receive funds from sponsoring companies, handle trademarks, provide infrastructure as necessary, support with developer relationships, industry and technical events, driving awareness, etc.
Governance	Understand and participate in the project's open governance processes and be an advocate for it.	When establishing new open source projects with industry partners, aim for a balanced governance that gives equal footing to all participants – a governance that welcomes contributors and supports a diverse community.	• Advise hosted projects on best open source governance models. • Help projects to implement their governance.
Access	Foster the culture of free and equal access for everyone.		
Development	• Follow processes. • Recommend improvements.	• Support new projects in creating a number of processes before they launch. These will change over time but it is a huge benefit to have something in place when projects kick off. • Recommend projects document their processes.	

	Open Source Developer	Open source Leadership	Open Source Foundation
Community Structure	• Support the right structure for the size of their project. • Recommend improvements based on their own experience participating in the project.	• Set the project governance and structure with growth and scale in mind. • Adopt practices that worked well in other projects. • Build in the ability to change as the project evolves.	
Releases	• Follow the release cadence when committing to deliver code for a given release. • Evangelize the importance of rhythmic releases. • Provide documentation for their contributions to support good release documentation.	• Promote a given release cadence. • Promote the need for release documentation. • Promote the need for a stable release. • Promote experimentation until the project figures out the right cadence and speed.	
Architecture	Design and implement with scale and growth in mind.	Promote a flexible and modular architecture.	
Communication tools	• Avoid private discussions. • Avoid participating in a closed communication medium (ML, IRC, etc.). • Be inclusive in your communication.	• Ensure that all newly launched or hosted projects offer communication tools used by typical open source projects and are platform agnostic. • Tools are available for anyone to use them and have access to all of the project's communication.	
Transparency	• The project has criteria to promote developers to key positions. • The project has a process that leads to making decisions. • The project has a process to accept incoming code from known entities. • Open communication channels. • Clear governance model.		

	Open Source Developer	Open source Leadership	Open Source Foundation
Development tools	• Use and promote the best open source tools available to support the project's development. • Mentor newcomers into the project on the use of the development tools adopted by the project.	• For any new open source projects your company creates, reply on open source development tools that are accessible to everyone.	• Ensure that all hosted project rely on development tools that are free and available to everyone.
Documentation	• Document your code. • Contribute documentation explaining architectural decisions, code structure, specific modules or features you have implemented, etc. • Review documentation contributed by others; provide feedback and ideas to improve on them. • Provide good headers within source code file. • Respect the project's coding practices and guidelines.	• Prioritize documentation as a parallel track to source code development. • Incentivize developers to provide documentation. • Sponsor interns or technical writers to create documentation for open source projects. • Ensure proper documentation that offer licensing and copyright information.	

Chapter 5

CLOSING

The open source methodology has proved itself over the past several decades that it is better to create software through collaboration and a transparent development process. Open source projects and initiatives provide companies with proven, successful models to collaborate with other companies, create new technologies, and support the development of new communities. Companies across many industries are creating Open Source Program Offices and staffing them with highly skilled individuals to help them drive open source software leadership and gain a critical footprint in this external R&D ecosystem. However, not all open source projects are equally open.

In this paper, we attempt to lay out best practices for open source openness and provide various indicators that may help you gauge the openness of an open source project. Some of these openness perspectives are visible from an external perspective and others are experienced more as a participant in the project.

The paper also provided recommendations on best–case openness scenarios for each of these indicators. If you are an open source developer, an open source leader in your organization, or a leader in an open source foundation, you can enable several best practices to ensure increased openness, transparency, diversity and inclusion in open source projects.

We hope this paper becomes a trigger for new conversations in open source projects on how to be more open, more transparent, and more inclusive.

References

Linux Foundation Enterprise Open Source Guides

https://www.linuxfoundation.org/resources/open-source-guides/

Software Package Data Exchange®

https://spdx.org/

The Software Package Data Exchange® (SPDX®) specification is a standard format for communicating the components, licenses and copyrights associated with software packages.

TODO Group

http://todogroup.org/

The TODO Group is a collection of tech companies who collaborate on the policies, practices, and pragmatics of running an open source program office. Their collaboration is managed as a community project under the Linux Foundation, and they are a resource to companies who are just starting to get their open source programs established.

CHAOSS Project

https://chaoss.community/

The Community Health Analytics Open Source Software project (CHAOSS) is a new Linux Foundation project focused on creating the analytics and metrics to help define community health. The project aims to establish standard implementation-agnostic metrics for measuring community activity, contributions, and health, which are objective and repeatable, and to produce integrated open source software for analyzing software community development.

ACKNOWLEDGMENTS

The author would like to express his sincere appreciation to Jessica Wilkerson (Director of Cybersecurity Research at the Linux Foundation), Christian Paterson (Head of Open Source Governance at Orange), Nithya Ruff (Head of Open Source Practice at Comcast) and Brian Warner (Program Director at the Linux Foundation) for their valuable reviews and feedback. The author is also especially grateful for feedback received from Steve Winslow (Director of Strategic Programs at the Linux Foundation) and the CHAOSS project with notable mention to Matt Germonprez, Kevin Lumbard and Georg Link. This paper has benefited immensely from the experiences and contributions of all reviewers.

FEEDBACK

Suggestions for improvement will be appreciated. Please send **comments** to the author directly.

DISCLAIMER

The opinions expressed in this paper are solely the author's and do not necessarily represent the views of current or past employers. The author would like to apologize in advance for any error or omission and is open for feedback and updates.

ABOUT THE AUTHOR

Ibrahim Haddad (Ph.D.) is the Executive Director of the **LF AI Foundation** that supports and sustains open source innovation in artificial intelligence, machine learning, and deep learning. He previously served as Vice President of R&D and Head of the Open Source Division at Samsung Electronics. At Samsung, he established the global open source division, set and executed Samsung's open source strategy, launched internal and external R&D collaboration projects, supported M&A and corporate VC activities, and represented Samsung in various foundations and consortia. Throughout his career, Haddad held several technology roles at Ericsson Research, the Open Source Development Lab, Motorola, Palm, Hewlett-Packard, and the Linux Foundation. He graduated with Honors from Concordia University (Montréal, Canada) with a Ph.D. in Computer Science, where he was awarded the J. W. McConnell Memorial Graduate Fellowship and the Concordia University 25th Anniversary Fellowship.

Twitter: **@IbrahimAtLinux**
Web: **IbrahimAtLinux.com**
LinkedIn: **linkedin.com/in/ibrahimhaddad**

Part IV

Patents in FOSS

Chapter 19

OIN License Agreement

OIN LICENSE AGREEMENT

Any Google Translate language translation provided for below is for convenience purposes only and shall not be of any legal force or effect. The Linux System definition is promulgated in English, and if there are any discrepancies, contradictions or inconsistencies between the Google Translate language translation and the original English language version, the interpretation under the original English language version shall govern and prevail.

Effective as of May 1, 2012.

This License Agreement ("Agreement") is entered into effective as of the last date of execution ("Agreement Date") between OPEN INVENTION NETWORK LLC, ("OIN"), and the undersigned Person ("You"). Words beginning with capital letters shall have the meaning set forth as noted in the body or in the definitions appended hereto.

SECTION 1. Licenses.

1.1 Subject to Section 1.2(b), OIN, grants to You and Your Subsidiaries a royalty-free, worldwide, nonexclusive, non-transferable license under OIN Patents to make, have made, use, import, and Distribute any products or services. In addition to the foregoing and without limitation thereof, with respect only to the Linux System, the license granted herein includes the right to engage in activities that in the absence of this Agreement would constitute inducement to infringe or contributory infringement (or infringement under any other analogous legal doctrine in the applicable jurisdiction).

1.2 Subject to Section 2.2 and in consideration for the license granted in Section 1.1, You, on behalf of yourself and your Affiliates, (a) grant to each Licensee and its Subsidiaries that are Subsidiaries as of the Eligibility Date a royalty-free, worldwide, nonexclusive, non-transferable license under Your Patents for making, having made, using, importing, and Distributing any Linux System; and (b) represent and warrant that (i) You have the full right and power to grant the foregoing licenses and the release in Section 1.4 and that Your Affiliates are and will be bound by the obligations of this Agreement; and (ii) neither You nor any of Your Affiliates has a Claim pending against any Person for making, having made, using, importing, and Distributing any Linux System. Notwithstanding anything in another Company Licensing Agreement to the contrary, You and your current and future Subsidiaries do not and shall not receive, and hereby disclaim and waive, any license from a Licensee and its current and future Affiliates pursuant to a Company Licensing Agreement for implementations of Linux Environment Components as specified in such Company Licensing Agreement to the extent that You and your current and future Affiliates are excepting any such implementations of Linux Environment Component from your license to a Licensee and its current and future Subsidiaries. The previous sentence is for the express benefit of the Members of OIN, OIN, and OIN's Licensees.

1.3 Subject to Section 1.2(b), OIN irrevocably releases You and Your Subsidiaries from claims of infringement of the OIN Patents to the extent such claims are based on acts prior to the Agreement Date that, had they been performed after the Agreement Date, would have been licensed under this Agreement.

1.4 You, on behalf of Yourself and Your Affiliates, irrevocably releases and shall release each Licensee and its Subsidiaries that are Subsidiaries on the Amendment Date and their respective Channel Entities and Customers that are Channel Entities and Customers, respectively, on or before the Amendment Date from any and all claims of infringement of Your Patents to the extent such claims are based on acts prior to the Amendment Date that, had they been performed after the Amendment Date, would have been licensed under this Agreement. As used herein, a Licensee's "Amendment Date" shall mean the later of the date an amendment becomes effective under Section 2.1 and the date such Licensee becomes a Licensee.

SECTION 2. Changes to Terms; Limitation of License

2.1 OIN may amend this Agreement, including the definitions on the OIN website, from time to time and will notify You in writing of any amendment at least sixty (60) days before the amendment becomes effective.

2.2 You may make a "Limitation Election" to limit Your patents that are subject to the license granted herein, effective on a "Limitation Date" thirty (30) days after giving written notice to OIN. If a Limitation Election is made, (a) OIN Patents, Licensee Patents, and Your Patents shall thereafter be limited to those licensable during the Capture Period, provided that the Capture Period with respect to Licensee Patents shall end on the Limitation Date; (b) the license in Section 1.1 will become limited to products and services made and marketed by You prior to the Limitation Date; (c) the definition of Linux System shall have the meaning as defined on the Limitation Date; (d) the license in Section 1.2 shall not extend to any Person that becomes a Licensee after the Limitation Date; and (e) any licenses granted in Company Licensing Agreements or any amendment by OIN executed after the Limitation Date shall not extend to You or Your Subsidiaries.

2.3 If through a change of control or otherwise, on a given date, You become unable to grant all the rights granted in Section 1.2, then: (a) the license granted in Section 1.1 shall terminate on such date; (b) the license granted in Section 1.2 and vesting prior to such date shall continue; and (c) for the purpose of this Section 2.3 only, the Capture Period as to OIN Patents, Licensee Patents, and Your Patents shall end on said date.

SECTION 3: Term of Agreement; Termination; Suspension

3.1 The term of this Agreement shall be from the Agreement Date until the last to expire of the OIN Patents or Your Patents, unless earlier terminated.

3.2 If a Subsidiary of You ceases to be a Subsidiary on a given date, the license granted in Section 1.1 to such Subsidiary shall terminate on such date. If an Affiliate of You ceases to be an Affiliate on a given date, the license granted in Section 1.2 and vesting prior to such date by such Affiliate shall continue.

3.3 If a Licensee or its Affiliate files one or more Claims against You or Your Subsidiaries based on products that perform substantially the same function as the Linux System, and are Distributed by You or Your Subsidiaries, then You may suspend the license granted under Section 1.2 to such Licensee and its Subsidiaries on written notice to such Licensee. Such suspension shall be effective unless and until such Claim is dismissed.

3.4 The license in Section 1.1 shall terminate effective on the day You or Your Subsidiary files one or more Claims against any Licensee, whose license has not been suspended by You under Section 3.3, for making, having made, using, importing, or Distributing any Linux System.

3.5 No termination or suspension of the licenses granted hereunder shall relieve either party of any obligation accrued hereunder prior to such termination.

SECTION 4: Notice

Notices and other communications in connection with this Agreement shall be in writing and signed by the party giving such notice, and shall be deemed to have been given upon receipt or upon tender to an appropriate individual at the following address:

For You and Your Subsidiaries:
SAMPLE COMPANY NAME

Subsidiary 1
Subsidiary 2
Subsidiary 3

For OIN:

The current OIN address as of the date of notice as specified on www.openinventionnetwork.com.

You shall copy OIN on all notices given in connection with this Agreement. Each party shall have both the unilateral right and the obligation to amend this Section 4 to keep its contact information current.

SECTION 5. Miscellaneous

5.1 No patents subject to this Agreement shall be assigned or any rights granted hereunder unless such assignment or grant is made subject to the terms of this Agreement. Neither OIN nor You shall assign this Agreement, assign any of its rights under this Agreement, or delegate any of its obligations hereunder, unless otherwise agreed in writing by the other party. Any attempt to do any of the foregoing shall be void.

5.2 OIN represents and warrants that it has the full right and power to grant the license set forth in Section 1. Except as provided in Section 1.2, neither party makes any other representations or warranties, express or implied.

5.3 This Agreement shall not affect any provision in other patent license agreements between You or Your Affiliates and any third party.

5.4 The parties acknowledge that some portions of the Linux System are subject to versions 1 and 2 of the GNU General Public License ('GPL') and that nothing in this Agreement is intended to cause a party not to comply with the GPL with respect to the Linux System. To the extent a provision of this Agreement would cause Licensee not to be in compliance with the GPL, such provision shall be interpreted in a manner consistent with the relevant version of the GPL, including that the Licensee shall be deemed to have received or granted any additional licenses required for compliance with that version of the GPL.

5.5 Each Licensee shall be a third party beneficiary of this Agreement with the right to enforce the terms and conditions of this Agreement directly against You and Your Affiliates.

5.6 This Agreement shall be construed in accordance with the laws of the State of New York as such laws apply to contracts entered into and fully performed in the State of New York.

This Agreement embodies the entire understanding of the parties with respect to the subject matter hereof, and replaces any prior or contemporaneous oral or written communications or agreements between them with respect to such subject matter.

Agreed to:

SAMPLE COMPANY NAME

Agreed to:

OPEN INVENTION NETWORK LLC

Definitions:

"Affiliate" shall mean, with respect to any specified Person, any other Person that now or in the future (i) is a Subsidiary of the specified Person, (ii) is a parent of the specified Person or (iii) is a Subsidiary of a parent of the specified Person. In each of the foregoing cases, such other Person shall be deemed to be an Affiliate only during the time such relationship as a Subsidiary or parent exists.

"Capture Period" shall mean the period beginning on the Agreement Date and ending on the earlier of (i) the date this Agreement or the license in Section 1.1 is terminated and (ii) the Limitation Date (as defined in Section 2.2), provided however, when You exercise a Limitation Election (as defined in Section 2.2), the Capture Period as to Your Patents shall end one year after the Limitation Date.

"Channel Entity", as to a Person, shall mean a direct or indirect distributor, reseller or re-licensor of such Person or other entity in such Person's sales or distribution channel.

"Claim" shall mean a lawsuit, binding arbitration, or administrative action, or other filed legal proceeding, including a counterclaim or cross-claim, alleging patent infringement.

"Company Licensing Agreement" shall mean a license agreement (including this Agreement) between OIN and another Person that has substantially the same terms and conditions as this Agreement, or a license agreement between OIN and a Member of OIN, designated by OIN as a Company Licensing Agreement.

"Customer", as to a Person, shall mean an end-user or other customer, direct or indirect, of such Person.

"Distribute" shall mean lease, license, offer to sell, sell, or otherwise provide, by any distribution means.

"Eligibility Date" shall mean, with respect to any particular Licensee, the later of the Agreement Date and the date such Licensee becomes a Licensee,

"Licensee" shall mean at any time, now or in the future, any Person other than You and your Subsidiaries that is granted a license under OIN Patents pursuant to a Company Licensing Agreement which license has not been terminated and with respect to which license said Person has not made a Limitation Election, or undergone a change in control in accordance with Section 2.3, prior to the Agreement Date.

"Licensee Patents," shall mean patents licensed by any and all Licensees pursuant to a Company Licensing Agreement.

"Linux System" shall, at any time, have the meaning set forth, at that time, on www.openinventionnetwork.com.

"Member of OIN" shall mean a Member of the Open Invention Network LLC as identified on the OIN website.

"OIN Patents" shall mean all patents and patent applications including utility models and typeface design patents and registrations, under which OIN has at any time during the Capture Period, the right to grant licenses to You or Your Subsidiaries

of or within the scope granted herein without such grant or the exercise of rights thereunder resulting in the payment of royalties or other consideration by OIN to unaffiliated third parties. OIN Patents shall include divisionals, continuations and continuations-in-part, results of reexaminations, any foreign counterparts of the foregoing patents and patent applications and any patents reissuing on any of the foregoing patents.

"Person" includes any individual, corporation, association, partnership (general or limited), joint venture, trust, estate, limited liability company or other legal entity or organization.

"Subsidiary" shall mean, with respect to any specified Person, any other Person of which more than 50% of the total voting power is owned or controlled, directly or indirectly, now or in the future, by the specified Person, but such other Person shall be deemed to be a Subsidiary only during the time such ownership or control exists.

"Your Patents" shall mean all patents and patent applications including utility models and typeface design patents and registrations (but not including any other design patents or registrations), under which You or any of Your Affiliates has at any time during the Capture Period, the right to grant rights of or within the scope granted herein without such grant or the exercise of rights thereunder resulting in the payment of royalties or other consideration by You or Your Affiliates to unaffiliated third parties (other than payments to third parties for patents or patent applications on inventions made by the third parties while employed by or providing services to You or any of Your Affiliates). Your Patents shall include divisionals, continuations and continuations-in-part, results of reexaminations, and any patents reissuing on, any of the foregoing patents, and any foreign counterparts of the foregoing patents and patent applications.

For existing OIN licensees, this license agreement is amended, effective May 1, 2012. Any licensee that entered into a license prior to the amendment, and that would like to receive a copy of the license agreement that was in effect at the time it originally signed its license, may request a copy by contacting OIN at info@openinventionnetwork.com.

What people are saying...

"At JD.com, we have employed open source technologies such as Kubernetes and Open Stack, along with Linux, to improve the speed, functionality and stability of our infrastructure while lowering operating costs."

– Rain Long, Chief Human Resource Officer & General Counsel, JD.com

Recently Joined the OIN Community

Open Invention Network
Research Triangle Park Center
4819 Emperor Blvd., Suite 400
Durham, NC 27703

info@openinventionnetwork.com

P +1 919.313.4902
F +1 919.313.4905

Chapter 20

The Truth About OSS-FRAND: By All Indications Compatible Models in Standards Settings (David J. Kappos and Miling Y. Harrington)

THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XX STLR.ORG SPRING 2019

COMMENT

THE TRUTH ABOUT OSS-FRAND: BY ALL INDICATIONS, COMPATIBLE MODELS IN STANDARDS SETTINGS†

David J. Kappos; Miling Y. Harrington*

Open source software ("OSS") has inevitably found its way into standards that contain standard essential patents ("SEPs"). However, some questions remain as to whether OSS licensing is inherently compatible with the FRAND licensing ("fair, reasonable, and non-discriminatory") that governs SEPs. Some argue that a license's compliance with the Open Source Initiative's "Open Source Definition" ("OSD") has always been understood to preclude patent royalties for the licensor by implicitly granting patent rights to the licensee. This Comment examines the historical record and finds no significant support for the notion that OSD-compliant licenses generally convey patent rights and thus preclude patent royalties.

* David J. Kappos is a partner in the Corporate Department of Cravath, Swaine & Moore LLP and previously served as the Under Secretary of Commerce and Director of the United States Patent and Trademark Office. Miling Y. Harrington is an associate in Cravath's Corporate Department.

I. INTRODUCTION

Recent decades have witnessed unparalleled technological achievements in the telecommunications, consumer electronics, and now, autonomous vehicle space with a pace of innovation that only continues to accelerate. Both open source software ("OSS") and standard essential patents ("SEPs") have been integral structural supports for this innovation. The associated policies of standard development organizations ("SDOs"), such as FRAND ("fair, reasonable, and non-discriminatory") licensing, ensure that the best technology is adopted into standards, allowing implementers to create standardized and interoperable products for consumers at reasonable prices. For its part, OSS innovation has progressed at breathtaking speed, significantly due to the strong social network of the OSS community and its ethos of sharing. As innovative products evolved to encompass the most cutting-edge IP, it was only natural that OSS would find its way into standards. However, some questions remain as to whether OSS is inherently compatible with FRAND licensing.

In the ongoing debate over open source licenses and their integration with SEPs governed by FRAND licensing (a debate termed "OSS-FRAND"), two arguments are often presented against the application of FRAND to open source: (1) FRAND licensing is detrimental for innovation, and (2) open source licenses are inherently incompatible with FRAND licensing. As we have previously discussed, neither of these propositions is correct.[1] Now, a third argument has been raised against FRAND policies which says that compliance with the Open Source Definition ("OSD") has always been understood to preclude patent royalties.[2] We examined the historical record to understand whether such a generalization could be made about the open source community. Before we turn

1. David J. Kappos, *Open Source Software and Standards Development Organizations: Symbiotic Functions in the Innovation Equation*, 18 COLUM. SCI. & TECH. L. REV. 259, 266-67 (2017), http://www.stlr.org/download/volumes/volume18/kappos.pdf.

2. *Ensuring Openness Through and In Open Source Licensing*, OPEN SOURCE INITIATIVE (Oct. 30, 2017, 3:25 PM), https://opensource.org/node/906.

to the evidence that this concept was neither widely accepted nor frequently discussed, let us first unpack the background and reasoning behind why some think OSD-compliant licenses and patent royalties cannot coexist and explain why that view is incorrect.

II. THE OSD DOES NOT ADDRESS PATENT RIGHTS

The Open Source Initiative, an organization that serves as an arbiter of acceptable open source licenses, maintains a set of parameters (the Open Source Definition or OSD), which must be satisfied for a license to be considered an open source license.[3] The OSD covers distribution, derived works, source code and non-discrimination, among other license parameters. OSD's Section 1 ("OSD 1") and Section 7 ("OSD 7") impose requirements for free redistribution. OSD 1 requires that "the license shall not require a royalty or other fee for such sale."[4] OSD 7 concerns distribution of licensed software and states that "[t]he rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties," precluding the execution of a separate license that would include royalties.[5] There is no doubt that OSD-compliant licenses are designed to cover copyright, and by extension, copyright royalties are not permitted. However, nowhere in the OSD does it state that an OSD-compliant license also conveys a patent grant.

III. THE OSI ARCHIVES DO NOT EVIDENCE CONSENSUS ON PATENT RIGHTS

Despite the lack of any actual indication of an intention to convey patent rights, some advocates contend that an implied patent license exists in OSD-compliant licenses, thereby creating an OSD 1 and OSD 7–based conflict with patent royalties contemplated by OSS-FRAND. Nonetheless, the question of whether the open source community generally had reached this consensus remained open. We set out to learn whether there is evidence to support an assertion of community consensus. We found no such consensus.

To remind ourselves of the conversations surrounding OSD-compliance and free redistribution accompanying OSS, we

3. *The Open Source Definition (Annotated)*, OPEN SOURCE INITIATIVE, https://opensource.org/osd-annotated (last visited Oct. 5, 2018).

4. *Id.*

5. *Id.*

examined all OSI License Discuss and License Review archives available from April 1999 to June 2018 for discussions mentioning OSD 1 or OSD 7.[6] We found that the community primarily discussed OSD 1 or OSD 7 in the context of analyzing whether specific licenses were OSD-compliant, with scant reference to patents. In over one hundred separate mentions each of OSD 1 and OSD 7 in the License Discuss archives, only seven of these instances contemplated OSD-compliant licenses to include a patent license. Likewise, we encountered around forty mentions of OSD 1 and sixty mentions of OSD 7 in the License Review archives, only six of which supported the view that OSD-compliant licenses include a patent license. Furthermore, these views were contemporaneously challenged. For example, two of the six License Review mentions supporting the patent license view occurred in an April 8, 2009 thread where the opposing position was also presented.[7] However, there is no indication that a consensus view emerged within the community following this discussion. Even as recently as 2017, the License Discuss lists continued to debate whether the OSD generally covered intellectual property rights beyond copyright.[8] With around a dozen mentions (less than 4%) of OSD 1/OSD 7 requiring patent licensing out of over 300 discussions directed specifically to the OSD 1/OSD 7 licensing issues, and no conclusion of any kind being reached or even proposed, we cannot conclude that any "consensus" was reached. If anything, the data suggest the opposite conclusion—that the issue of patents was not assumed or overlooked; it was affirmatively raised by a few outliers; it did not get traction with the community; and like many other outlier comments, it was left unadopted, deemed rejected by omission.

IV. THERE IS NO IMPLIED LICENSE IN OSD

The view that a patent license can be implied from an OSD-compliant license seems to be rooted in a theory of legal estoppel.

---

6. *See The License-review Archives*, OPEN SOURCE INITIATIVE, http://lists.opensource.org/pipermail/license-review_lists.opensource.org/ (last visited Mar. 8, 2019); *The License-discuss Archives*, OPEN SOURCE INITIATIVE, http://lists.opensource.org/pipermail/license-discuss_lists.opensource.org/ (last visited Mar. 8, 2019).

7. *See* Matthew Flaschen, *For Approval: MXM Public License*, OPEN SOURCE INITIATIVE (Apr. 8, 2009, 3:50 PM), http://lists.opensource.org/pipermail/license-review_lists.opensource.org/2009-April/000717.html.

8. *See* Christopher Sean Morrison, *Patent Rights and the OSD*, OPEN SOURCE INITIATIVE (Mar. 6, 2017, 11:41 PM), http://lists.opensource.org/pipermail/license-discuss_lists.opensource.org/2017-March/019813.html.

Proponents turn to *TransCore LP v. Electronic Transactions Consultants Corp.* for judicial support.[9] However, *TransCore* is inapposite to the OSD license context. The *TransCore* court found that a covenant not to sue on an earlier-issued patent as part of a settlement agreement created an implied patent license to a later-issued, related patent, and the patent-holder was legally estopped from suing for infringement of the later-issued patent. Regarding legal estoppel, the court stated: "The basic principle is, therefore, quite simple: 'Legal estoppel refers to a narrow [] category of conduct encompassing scenarios where a patentee has licensed or assigned a right, received consideration, and then sought to derogate from the right granted.'"[10] *TransCore* clearly involved patent rights and a patentee to begin with, unlike the OSD license context, which is rooted in an affirmative copyright grant and no patent grant. The OSD context also does not lend itself to a "narrow category of conduct." To the contrary, implying a patent licensee based on a free, unsigned, automatic copyright license would sweep in a broad array of conduct. Furthermore, although the Federal Circuit discussed legal estoppel in *Wang Laboratories, Inc. v. Mitsubishi Electronics America, Inc.*, 103 F.3d 1571, 1581 (Fed. Cir. 1997), its ultimate finding of an implied patent license was rooted in equitable rather than legal estoppel.[11] While legal estoppel analysis looks for "an affirmative grant of consent or permission to make, use, or sell; i.e. a license," equitable estoppel analysis "focuses on 'misleading' conduct suggesting that the patentee will not enforce patent rights."[12] Equitable estoppel has even less of a basis to be applied broadly to OSD licenses as a class.

Our research was unsuccessful in finding any court case that has considered whether patent licenses are implied by open source licenses in the absence of express language. But the case law

---

9. *See* Christian H. Nadan, *Closing the Loophole: Open Source Licensing & the Implied Patent License*, 26 COMPUTER & INTERNET LAW. 1, 3 (2009) (citing TransCore, LP v. Elec. Transaction Consultants Corp., 563 F.3d 1271 (Fed. Cir. 2009)).

10. TransCore, LP v. Elec. Transaction Consultants Corp., 563 F.3d 1271, 1279 (Fed. Cir. 2009) (quoting Wang Labs., Inc. v. Mitsubishi Elecs. Am., Inc., 103 F.3d 1571, 1581 (Fed. Cir. 1997)).

11. Wang Labs., Inc. v. Mitsubishi Elecs. Am., Inc., 103 F.3d 1571, 1582 (Fed. Cir. 1997) (finding that Wang's behavior over six years, including repeatedly attempting to convince Mitsubishi to join the SIMMs market, providing Mitsubishi with designs, purchasing SIMMs from Mitsubishi, lobbying for Wang's design to become an industry standard, and receiving payment from Mitsubishi, was enough for Mitsubishi to infer that it had obtained consent to use Wang's patents).

12. *Id.* at 1581.

surrounding implied licenses indicates that courts are hesitant to imply a license where one is not expressly set forth. In the recent case *Endo Pharmaceuticals Inc. v. Amneal Pharmaceuticals, LLC*, 224 F.Supp.3d 368 (D. Del. 2016), the District of Delaware quoted the Federal Circuit's statement in *Wang Laboratories*, that "judicially implied licenses are rare under any doctrine," in concluding that defendant Teva had not demonstrated facts supporting an implied patent license.[13] Likewise, the Northern District of California has stated, "Courts have found implied licenses only in narrow circumstances where one party created a work at [the other's] request and handed it over, intending that [the other] copy and distribute it."[14] The implied patent license inquiry in general is narrow and fact-specific,[15] and thus unsuited to any untethered genus, including OSD-compliant licenses as a class.

In summary, our research revealed no legal support for application of an implied patent license to OSD-compliant license agreements.[16] Instead, all extant case law, including recent court decisions, indicate that courts following precedent would be compelled to find against any implied patent license or any patent exhaustion theory in an OSD-compliant licensing context.

V. KEY LICENSE AUTHORS HAD NO EXPECTATION OF GRANTING PATENT RIGHTS

Given the lack of support for community consensus of a patent license during the early development of open source norms, and the lack of support in the case law, we surveyed the expectations of other

13. Endo Pharms. Inc. v. Amneal Pharms., LLC, 224 F.Supp.3d 368, 382 (D. Del. 2016) (quoting *Wang Labs., Inc.*, 103 F.3d at 1580).

14. Oracle Am., Inc. v. Terix Comput. Co., Inc., No. 5:13-CV-03385-PSG, 2015 WL 2090191, at *8 (N.D. Cal. May 5, 2015) (quoting A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1026 (9th Cir. 2001)).

15. *See, e.g.*, Brian Cook, *Clearing A Path for Digital Development: Taking Patents in Eminent Domain Through the Adoption of Mandatory Standards*, 82 S. CAL. L. REV. 97, 103 (2008).

16. Some have also argued that regardless of whether a patent license can be implied, the theory of patent exhaustion somehow applies in the OSS context, preventing a patent owner from asserting its patent against users of its distributed code and thereby precluding the receipt of patent royalties. Nadan, *supra* note 9, at 4 n.31. However, it is only "a patentee's decision to sell a product [that] exhausts all of its patent rights in that item." *Impression Prods., Inc. v. Lexmark Int'l., Inc.*, 137 S. Ct. 1523, 1529 (2017). Permitting one's software to be distributed under an OSS license that conveys no patent rights involves neither the selling of a product nor the licensing of a patent and does not implicate patent exhaustion. We are aware of no case that has found the exhaustion doctrine to apply in the circumstances involved with open source licenses.

important stakeholders. At the technology transfer offices of University of California, Berkeley and the Massachusetts Institute of Technology, institutions credited with starting the eponymous and immensely popular permissive licenses, BSD and MIT, respectively, the consensus is that these two licenses do not cross into patents. "MIT takes a pragmatic approach," said Daniel Dardani, MIT's chief software and information technology licensing officer. He continued:

> The words of the license do not include any mention of patents, so we do not view a patent license as being granted. In fact, as a general rule, the TLO has avoided using open source licenses with express patent grant language. To imply a patent grant from licenses that otherwise do not contain such express language would create potential conflicts given MIT's substantial and diverse portfolio of patented technologies, many of which are exclusively licensed to companies.[17]

This position is shared by Berkeley's Office of Technology Licensing (OTL). Curt Theisen, the Associate Director of the OTL, adds:

> The Berkeley OTL has never taken the position that the BSD includes a patent grant. In fact, we regularly advise our community members that the BSD license is an excellent OSS license to use because it permits broad licensing of software with minimal restrictions and maximum compatibility with other software and licenses.[18]

Both Berkeley's and MIT's views fit into the broader consensus that permissive licenses, unlike copyleft licenses, do not contain restrictive language and are compatible with FRAND licensing.[19] We are thus compelled to conclude that the view that certain OSD-compliant licenses necessarily grant patent rights, causing incompatibility with FRAND, is neither rooted in the past nor serves the interests of the present.

---

17. Personal communication with D. Dardani (Mar. 19, 2018).
18. Personal communication with C. Theisen (June 12, 2018).
19. Kappos, *supra* note 1.

VI. A FORCED OSS-FRAND FREE PATENT LICENSE DISTURBS THE INNOVATION ECOSYSTEM

Turning finally to the bigger picture, it is important to understand that OSD-compliant licenses in the context of OSS-FRAND cannot be examined in isolation. The software they cover is integrated into highly sophisticated products (such as smartphones) that encompass intellectual property covering myriad functions and components. To declare OSD-compliant licenses to be incompatible with patent royalties both over-extends the reach of the software license to functions and components beyond the scope of the license, and "solves" a problem that is already amply addressed by existing safeguards.

Given the integration of open source software into widely varying products containing innovations beyond the software, an implied patent license to the software inherently extends to those further innovations. This creates the unavoidable consequence of open source software undermining patent rights well beyond the software—an extreme result that could not have been intended or contemplated by anyone.

Moreover, such a measure is not necessary to protect SEP implementers from unfair royalties. For one, OSS authors who wish to extend a patent license already have the ability to do so through licenses like Apache 2.0 and GPL v3 that contain express patent license-granting language. Furthermore, the FRAND system of licensing, which is required by SDOs, mandates reasonable terms and conditions—including reasonable royalties, and requires treating similarly situated licensees similarly. This existing system achieves a balance between making technologies available to implementers at a reasonable cost and rewarding and incentivizing innovators. Also, it creates no structural barriers against the adoption of open source. In fact, integrating open source into the current standards regime is, as the European Commission puts it, a "win-win situation: on one side the alignment of open source and standardization can speed-up the standards development process and the take-up of . . . [standards] and on the other side standards can provide for interoperability of open source software implementations."[20]

Because we observed conflicting positions regarding whether OSD-compliant licenses grant patent rights, we decided to examine the facts and law behind them. We found no significant support for

20. *Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Setting out the EU approach to Standard Essential Patents*, COM (2017) 712 final (Nov. 29, 2017).

the notion that OSD-compliant licenses convey patent rights—neither in the form of case law nor community consensus. Instead, we found significant support for the opposite conclusion: that OSD-compliant licenses should not be assumed to grant patent licenses unless there is express language that states so. In short, an OSS licensor can choose to grant a patent license or, like MIT and Berkeley, choose not to do so, and preserve the ability for OSS and SEPs to work in tandem in advancing innovation.

Chapter 21

OSS and FRAND: Complementary Models for Innovation and Development (Van Lindberg)

THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XX STLR.ORG SPRING 2019

COMMENT

OSS AND FRAND: COMPLEMENTARY MODELS FOR INNOVATION AND DEVELOPMENT†

Van Lindberg*

In The Truth About OSS-FRAND, *David Kappos and Miling Harrington argue that it is both permissible and desirable to charge FRAND ("fair, reasonable, and non-discriminatory") royalties on open source software ("OSS") that is incorporated into a standard containing standard-essential patents ("SEPs"). In arguing that OSS and FRAND are compatible in this way, Kappos and Harrington take the position that when standard-setting communities intentionally incorporate OSS-licensed code into a standard, it is the royalty-free status of open source that should give way, not the payment of the FRAND-based royalty. This Comment examines the Open Source Definition ("OSD"), the text of OSD-compliant licenses, and discussions surrounding their creation to conclude, contrary to Kappos and Harrington, that essentially every OSD-compliant open-source license includes a royalty-free patent grant, which precludes the imposition of FRAND-based royalties. Standard-setting organizations that wish to charge FRAND royalties ultimately have the same option that commercial enterprises have when dealing with open source: respect OSD licenses, including their implied royalty-free patent grants, or create an alternative commercial license that conveys no patent grant.*

* Member at Dykema Gossett and General Counsel of the Python Software Foundation. J.D., B.S. Brigham Young University. Special thanks to Pamela Chestek for her insightful feedback, and to the staff of the *Columbia Science and Technology Law Review* for their patient and helpful review.

I. INTRODUCTION

A patent gives its owner the right to exclude others from making, using, or selling the claimed invention.[1] In contrast, open source licenses grant licensees broad permission to modify, compile, distribute, and use open source software ("OSS"). When open source software embodies or implicates patent claims, a patent holder's right to exclude is in tension with an open source licensee's permission to use and distribute the software freely.

1. 35 U.S.C. § 271(a) (2000) states: "Except as otherwise provided in this title, whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent."

In *The Truth About OSS-FRAND*,[2] David Kappos and Miling Harrington attempt to resolve this tension by arguing that it is both permissible and desirable to charge FRAND ("fair, reasonable, and non-discriminatory") royalties on open source-licensed code incorporated into a standard.[3] As Kappos and Harrington cast it, critics make three key arguments that they want to address and refute: "(1) FRAND licensing is detrimental for innovation (2) open source licenses are inherently incompatible with FRAND licensing, . . . [and (3)] compliance with the Open Source Definition (OSD) has always been understood to preclude patent royalties."[4] This is the second in a series of writings in which Kappos has advanced similar policy positions.[5] Regardless of the policy outcome that Kappos and Harrington may prefer, however, they fail to account for some cases and facts that collectively undermine the legal and historical argument that they are attempting to make.

I will not address the first argument that Kappos and Harrington work to refute–i.e. that "FRAND licensing is detrimental for innovation." Given the number of modern technologies that have evolved through the standards-setting process, I agree that FRAND-based standards setting is a successful model for promoting and commercializing innovation. I also agree with the numerous statements in Kappos' two articles recognizing that OSS is also a successful model for promoting innovation.[6] The deeper issue is whether these models are essentially "compatible," as Kappos and Harrington contend, or whether they are merely "complementary" alternatives. Put another way, we need to ask if a patent holder and open source licensor should be permitted to charge ongoing

---

2. David. J. Kappos and Miling Y. Harrington, *The Truth About OSS-FRAND: By All Indications, Compatible Models in Standards Settings*, 20 COLUM. SCI. & TECH. L. REV. 242 (2019), available at http://www.stlr.org/cite.cgi?volume=20&article=Kappos.pdf.

3. *Id.* (manuscript at 7).

4. *Id.* (manuscript at 2) (citations omitted).

5. David J. Kappos, *Open Source Software and Standards Development Organizations: Symbiotic Functions in the Innovation Equation*, 18 COLUM. SCI. & TECH. L. REV. 259, 267 (2017), http://www.stlr.org/download/volumes/volume18/kappos.pdf.

6. *See, e.g.*, Kappos & Harrington, *supra* note 2 (manuscript at 1) ("For its part, OSS innovation has progressed at breathtaking speed, significantly due to the strong social network of the OSS community and its ethos of sharing."); Kappos, *supra* note 5, at 261 ("Open Source Software also provides efficiencies and network effects crucial to innovation. Unlike proprietary software, OSS gives developers access to the source code of computer programs developed by others working on a given open source project, and enables developer communities to share tools and build on common infrastructure.")

royalties on OSS-licensed materials that embody patent claims, such as those incorporated into a FRAND-licensed standard.

This Comment argues that neither the licenses, nor the law, nor public policy supports such a position. Part II presents a simple model for evaluating open source licensing. Part III addresses the existence and implications of explicit patent licenses included in many open source licenses. Part IV evaluates the points made by Kappos and Harrington relating to the Open Source Definition. Finally, Part V discusses the complementary roles of OSS and FRAND licensing in promoting innovation.

II. MODELING OPEN SOURCE AS "FREE TRADE" IN INTELLECTUAL PROPERTY

Open source is a unique construct in intellectual property law. Rather than using intellectual property law to restrict the use of software, those same laws are used to guarantee the availability of OSS-licensed software to third parties. Some open source licenses accomplish this through broad, automatic licensing to all recipients. In other open source licenses, distributors are required to pass forward to all users the same permissions they received. These pass-forward licenses are sometimes referred to as "copyleft," a play on the all-rights-reserved orientation of copyright.

While one could consider open source licensing to be, in some sense, "just software licensing," a better mental model is that of a free trade agreement: Open source is a framework that allows people to share and trade intellectual property. This is different from traditional software licensing, where you typically trade intellectual property for money; with open source licenses you trade code—intellectual property—for other code.

A simple model of open source helps illuminate a number of unique factors associated with open source legal analysis. Let's consider what happens when someone writes some code and releases that code under an open source license:

1. Deborah Developer creates some software.
2. Deborah chooses an open source license and distributes the software under the license.
3. Larry Licensee receives a copy of the software and a copy of the license. The license includes a *grant* of permissions, and one or more *conditions* with which Larry needs to comply.
4. If Larry complies with the conditions, he also receives the right to distribute the software to other people.

Even though this model is simple, it hides tremendous legal complexity.

A. Open Source Licenses are Chosen, not Negotiated

The first thing to notice about this model is that Deborah *chooses* an open source license—she doesn't *create* an open source license. Most people don't realize that "open source" is a defined term. Deborah can't just write a new license and declare that the license is "open source." There is an organization, the Open Source Initiative ("OSI"), that certifies whether or not a license qualifies as an "open source license."[7] The OSI determines whether a license is open source by evaluating whether a proposed license conforms to a set of ten principles called the "Open Source Definition."[8] At the present time, there are only 81 accepted open source licenses.[9]

Thus, even though Deborah is the open source *licensor* (i.e., the party *granting* a license to her code), she did not draft the license[10] or negotiate its terms with Larry. Instead, she chose one of the 81 official open source licenses and adopted it, warts and all, as the license for her software.

The implication of this fact is that some typical canons of license interpretation may not apply in the open source context. There is no finely tuned negotiation. Instead, the licensor chooses an open source license that *most closely approximates* the terms desired and offers the software to any potential licensee on a "take it or leave it" basis.

B. Open Source Licenses are Designed to Maximize Distribution and Use

Open source software is designed to spread. Both by presenting favorable terms to licensees and by restricting the set of available licenses (and license terms), open source licenses maximize the ease

---

7. It is possible to create new licenses and have them certified by the OSI to be "open source." But creating a new open source license is a rare and time-consuming process, the details of which are not relevant to the arguments presented here.

8. *The Open Source Definition (Annotated)*, OPEN SOURCE INITIATIVE, https://opensource.org/osd-annotated (last visited Apr. 24, 2019).

9. *See Licenses by Name*, OPEN SOURCE INITIATIVE, https://opensource.org/licenses/alphabetical (last visited Apr. 24, 2019) (list of licenses currently approved by OSI).

10. For information on who originally wrote various licenses, see *Comparison of free and open-source software licenses*, WIKIPEDIA, https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses (last visited Apr. 24, 2019).

of distribution and minimize the friction associated with ordinary license negotiations. Open source licenses are also self-executing,[11] meaning that each person who receives a copy of the covered work is automatically granted a new license upon receipt.

In practice, this means that open source licenses are evaluated using a unilateral contract model. The software is made available under fixed license terms by the licensor, and a licensee indicates acceptance of the license by acting in a manner authorized by the license. In the context of open source licenses, almost any act by a potential licensee is enough to "accept" the license, causing it to attach. No specific performance other than receiving, using, or distributing the software is required.[12]

C. Open Source Licenses are Legal Documents, but Commentary and Context Provide Clues to Interpretation

The scope of an open source license is evaluated just as with any other software license: by examining what is present within the "four corners" of the license document. The text of a particular license is the most important factor in understanding the scope of any license grants.

The problem is that many of the original open source licenses were not written by lawyers, but instead by engineers looking to maximize the use of their software. These engineer-written licenses may not reflect common legal usage.

Many open source licenses are also old, with many frequently-used licenses dating back two or three decades. For example, the first version of one widely-used license, the GNU General Public License, was originally released in 1989. These older licenses sometimes reflect legal understandings that were current when the license was written—not what is understood now.

However, there is a benefit to the history surrounding open source: there are many documents and public analyses that can be used to resolve ambiguous elements in the licenses and to understand the usage of trade that surrounds open source licenses.

---

11. *See, e.g.*, Section 10 of the GNU General Public License, version 3: 10. *Automatic Licensing of Downstream Recipients*, https://www.gnu.org/licenses/gpl-3.0.en.html ("Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License.").

12. *See, e.g.*, RealNetworks Public Source License Version 1.0 (RPSL-1.0), https://opensource.org/licenses/RPSL-1.0 ("You are not required to accept this License. However, nothing else grants You permission to use, copy, modify or distribute the software or its derivative works.").

The most important of these public analyses is the Open Source Definition. The OSD was the result of a concerted effort to consolidate and standardize common usage around the meaning of the term "open source."[13] The OSD stands out as an interpretive aid because it codifies common principles that apply to *all* open source licenses. Each time a new open source license is proposed, the OSI shepherds a public evaluation of the proposed license, and ultimately votes whether or not to certify the license as "open source." Thus, the OSD and the actions of the OSI can be given some interpretative weight in evaluating what both parties understood about the scope of an open source license grant.

III. WITHIN THE "FOUR CORNERS" OF OPEN SOURCE LICENSES

Returning to the arguments advanced by Kappos and Harrington, the majority of their analysis focuses on: (1) examining the text of the OSD,[14] (2) reviewing licensing discussions in the OSI's archives,[15] and (3) evaluating statements from the technology licensing offices at the Massachusetts Institute of Technology and University of California, Berkeley, the "stewards" and original "institutional" authors of the MIT and BSD licenses, respectively.[16] Using these tools, Kappos and Harrington argue that there is no historical consensus supporting the argument that a patent owner is precluded from imposing patent royalties on software released with an OSD-compliant open source license.[17]

I agree that the OSD is relevant, and Kappos and Harrington's work analyzing the OSD is valuable. As noted above, the principles from the OSD apply to every open source license. Thus, they represent a shared understanding about *all* open source licenses, and can be used to illuminate the "meeting of the minds" between the licensor and the licensee to the extent it exists.[18] However, the primary interpretive effort should be centered on the text of the

13. *See History of the OSI*, OPEN SOURCE INITIATIVE, https://opensource.org/history (last updated Oct. 2018).

14. Kappos & Harrington, *supra* note 2 (manuscript at 2-3).

15. *Id.* (manuscript at 3-4).

16. *Id.* (manuscript at 6-7).

17. *Id.* (manuscript at 2).

18. The comments of the license stewards are interesting but of questionable relevance. *See id.* (manuscript at 6-7). A court would not give private, hearsay statements by non-parties any interpretive weight. Even in terms of historical understanding, the individuals quoted were not present when these licenses were created by their institutions, and no one presents any evidence that they have special historical insight.

licenses themselves. But under standard canons of license interpretation, parol evidence is primarily useful for guiding interpretation when the text of the license itself is ambiguous—and I submit that there is less ambiguity in open source licenses than would first appear.

To set the terms of the debate, the key question is whether all open source licenses include a royalty-free patent license. This key question can be further subdivided into two related questions:

1) Do all open source licenses include a patent grant?

2) Do all open source licenses specify royalty-free terms?

Separating the key question in this way allows for a substantial simplification of the debate. The first principle of the OSD (henceforth "OSD 1") specifies that all open source licenses allow for "Free Redistribution" and states that the license "shall not restrict any party from selling or giving away the software. . . . The license shall not require a royalty or other fee for such sale."[19] For their part, Kappos and Harrington appear to agree that all open source licenses allow for royalty-free redistribution.[20] Thus, question #2 is answered in the affirmative: all open source licenses require royalty-free terms.

Thus, the focus of this Comment is on question #1—whether all open source licenses include a patent grant. Kappos and Harrington argue that they do not;[21] I argue that they do.

In the analysis below, I discuss three types of patent grants that apply to open source licenses: "classical" patent grants, "express"

19. The full text of the first principle of the OSD reads: "1. Free Redistribution: The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale. *Rationale: By constraining the license to require free redistribution, we eliminate the temptation for licensors to throw away many long-term gains to make short-term gains. If we didn't do this, there would be lots of pressure for cooperators to defect.*" *The Open Source Definition (Annotated)*, OPEN SOURCE INITIATIVE, https://opensource.org/osd-annotated. (last visited Apr. 24, 2019).

20. Kappos & Harrington, *supra* note 2 (manuscript at 2) ("Section 1 (OSD 1) and Section 7 (OSD 7) of the OSD impose requirements for free redistribution."); *id.* (manuscript at 3) ("To remind ourselves of the conversations surrounding OSD-compliance and free redistribution attendant OSS . . . .").

21. *Id.* (manuscript at 3) ("However, nowhere in the OSD does it state that an OSD-compliant license also conveys a patent grant."); *id.* (manuscript at 4) ("*TransCore* clearly involved patent rights and a patentee to begin with, unlike the OSD license context which is rooted in an affirmative copyright grant and no patent grant.").

patent grants, and implied patent licenses.[22] Because there are only 81 licenses, it is possible to exhaustively review every open source license for evidence of a patent grant. Having done so, I conclude that essentially every open source license includes a patent grant.

A. "Classical" Patent Grants

The first type is what I will refer to as a "classical" patent grant, because this is the type of patent grant that appears in most commercial license agreements. A classical patent grant explicitly uses terms like "patent grant" or "patent license" and echoes the words used in the patent statute to describe a patent holder's exclusive rights: make, use, sell, offer to sell, and import.[23] For example, from the Academic Free License:

> Grant of Patent License. Licensor grants You a worldwide, royalty-free, non-exclusive, sublicensable license, under patent claims owned or controlled by the Licensor that are embodied in the Original Work as furnished by the Licensor, for the duration of the patents, to make, use, sell, offer for sale, have made, and import the Original Work and Derivative Works.[24]

There doesn't seem to be any disagreement, including from Kappos and Harrington, that these classical patent grants are effective, and that an open source license that contains a classical patent grant is incompatible with FRAND licensing.[25]

B. "Express" Patent Grants

The second type of patent grant is what I will call an "express" patent grant, of which there are two types.

---

22. *N.B.*: Only the phrase "implied patent license" is a term of art. The categorization of other grants as "classical" or "express" is used here for clarity in referring to different styles of wording a patent grant.

23. 35 U.S.C. § 271(a) (2000); *see also* 35 U.S.C. § 154(a)(1) (2015).

24. Lawrence Rosen, *Academic Free License ("AFL") Version 3.0* (2005), https://opensource.org/licenses/AFL-3.0 (last visited Apr. 24, 2019).

25. *See, e.g.*, Kappos & Harrington, *supra* note 2 (manuscript at 7) ("OSS authors who wish to extend a patent license already have the ability to do so through licenses like Apache 2.0 and GPL v3 that contain express patent license grant language.").

1. Conventional Express Patent Grants

A conventional express patent grant does not include a term such as "patent grant" or "patent license," but the license explicitly grants permission for the licensee to exercise one or more of the rights reserved to a patent owner: to make, use, sell, offer to sell, or import. For example, from the MIT license:

> Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the ***rights to use***, copy, modify, merge, publish, distribute, sublicense, and/or *sell* copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
>
> The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.[26]

Similarly, the BSD license:

> Redistribution and *use*, with or without modification, are permitted provided that the following conditions are met . . .[27]

Admittedly, most agreements that grant patent licenses use the term "patent." But if a licensor grants someone permission to "use" or "sell" something, that is a patent license, even though the word "patent" isn't included in the license text. The licenses that have "express" patent grants include an explicit grant of the right to "use" the software. Many licenses, like the MIT license, also grant other patent-denominated rights like the right to "sell."

Courts have held that agreements that do not contain the word "patent" still may create a patent license if the patentee grants another party the ability to exercise one of the exclusive rights reserved to the patent holder under the statute.[28] For example, in

---

26. *The MIT License*, OPEN SOURCE INITIATIVE, https://opensource.org/licenses/MIT (last visited Apr. 24, 2019) (emphasis added).

27. *The 2-Clause BSD License*, OPEN SOURCE INITIATIVE, https://opensource.org/licenses/BSD-2-Clause (last visited Apr. 24, 2019).

28. *In re* Davidson Hydrant Techs., Inc., No. 11-13349-WHD, 2012 Bankr. LEXIS 1120, at *14 (Bankr. N.D. Ga. Jan. 10, 2012) ("[T]he authorization to offer

Viam Mfg., Inc. v. Iowa Exp.-Import Trading Co., the Federal Circuit held that a "Marketing Agreement" that stated "[the patentee] agrees to supply Products to [the licensee] for sale in North America" created a patent license.[29] The Eleventh Circuit Bankruptcy Court cited *Viam* when analyzing another case, holding that the specific use of the term "sale" was significant, as the right to sell is exclusively reserved to patentees.[30]

2. GPL-Style Express Patent Grants

Another type of express patent grant is exemplified by the language in a broadly-used open source license called the GNU General Public License, version 2 ("GPLv2"). The GPLv2 is unusual in that it *mentions* patents, but does not include a classical patent grant. Instead, there is broad and ambiguous language regarding patent rights in general. While the GPLv2 states that "[t]he act of running the Program is not restricted," additional statements suggest that patent licenses might be required, but should be freely available. For example, the Preamble states: "We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all."[31]

This is one of the few occasions in open source law where there is a ruling from a court directly on point. Although Kappos and Harrington indicate that they were "unsuccessful in finding any court case that has considered whether patent licenses are implied by open source licenses in the absence of express language,"[32] this exact issue was discussed and decided in the context of a 12(b)(6) motion in *XimpleWare, Inc. v. Versata Software, Inc.*[33] In *XimpleWare*, a patent holder and GPL licensor accused both Versata and Versata's customers of patent infringement. As stated by the court, "Because

---

the products for sale without being subject to suit for infringement of Debtor's patent constitutes the license of a right in the patent.").

29. Viam Mfg., Inc. v. Iowa Exp.-Import Trading Co., 99-1280, 00-1038, 2000 U.S. App. LEXIS 22443, at *5 (Fed. Cir. Aug. 31, 2000).

30. *In re* Davidson Hydrant Techs., Inc., 2012 Bankr. LEXIS 1120, at *20-21 ("[It] does appear that the marketing agreement at issue in Iowa Export-Import differed from the Agreement in at least one key way. The Iowa Export-Import agreement clearly used the word 'sale,' whereas the Agreement does not.").

31. GNU Project, GPLv2 Preamble (1991), https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html; *cf.* Section 7.

32. Kappos & Harrington, *supra* note 2 (manuscript at 5).

33. XimpleWare, Inc. v. Versata Software, Inc., 2014 U.S. Dist. LEXIS 68515 (N.D. Cal. 2014).

an *express license* is a defense to patent infringement, XimpleWare's direct infringement claims against Versata's customers turn on *whether the customers' distribution is licensed under the GPL*."[34] The *XimpleWare* court went on to find that because Versata's customers had not distributed the GPL-licensed software in a way that violated the license terms, they had a valid license under the GPLv2—and under XimpleWare's patents.

3. Totaling It Up: Patent Grants in OSS

Between classical patent grants, conventional express patent grants based on permissions to "use" or "sell" the software, and GPLv2-style express patent grants, almost every open source license is accounted for. Of the 81 licenses certified as open source, all but three include either a classical patent grant or express patent grant including at least the right to "use" the software. The three exceptions are in a family of licenses (the *Licences Libre du Québec*) that are not written with reference to US law.[35]

Thus, if effectively every open source license includes some kind of patent grant, the question turns from whether there *is* a patent grant to the *scope* of the grant provided. At that point, having

34. *Id.* at *15 (emphasis added).

35. OSI currently accepts 81 licenses as open source. *See Licenses by Name*, OPEN SOURCE INITIATIVE, https://opensource.org/licenses/alphabetical (last visited Apr. 24, 2019).

Of those 81: (a) 38 include a classical patent grant; (b) 32 contain an express grant to "use" the software, and sometimes include other rights, such as the rights to "sell"; (c) three are the Licences Libre du Québec; and (d) five adopt language from the GPLv2, which states that "any patent must be licensed for everyone's free use" grants all rights needed for "running" the program, and specifies that "you can change the software or use pieces of it in new free programs." By category, the licenses are as follows (using SPDX Short Identifiers where applicable):

Classical patent grant: AFL-3.0, AGPL-3.0, APL-1.0, APSL-2.0, Apache-2.0, Artistic-2.0, BSD-2-Clause-Patent, CATOSL-1.1, CDDL-1.0, CECILL-2.1, CPAL-1.0, ECL-2.0, EPL-1.0, EPL-2.0, EUPL-1.2, GPL-3.0, IPL-1.0, LGPL-3.0, LPL-1.02, MPL-1.0, MPL-1.1, MPL-2.0, MS-PL, MS-RL, Motosoto, NASA-1.3, NPOSL-3.0, Nokia, OCLC-2.0, OSET, OSL-3.0, RPL-1.5, RPSL-1.0, RSCPL, SPL-1.0, UPL, Upstream, Watcom-1.0;

Conventional express grant to "use" or more: 0BSD, 0BSD, AAL, BSD-2-Clause, BSD-3-Clause, BSL-1.0, CNRI-Python, EFL-2.0, EUDatagrid, Entessa, Fair, Frameworx-1.0, HPND, IPA, ISC, MIT, MirOS, Multics, NCSA, NGPL, NTP, Naumen, OFL-1.1, OGTSL, PHP-3.0, PostgreSQL, Python-2.0, QPL-1.0, SimPL-2.0, Sleepycat, VSL-1.0, W3C, Xnet, ZPL-2.0, Zlib;

GPLv2 language: GPL-2.0, LGPL-2.1, LPPL-1.3c, WXwindows, eCos; and

International Licenses (Licences Libre du Québec): LiLiQ-P, LiLiQ-R, LiLiQ-R+.

established the existence of a patent grant, it is not too hard to find patent rights implicated within the grant, even if such grants are expressed in copyright terms. For example, the right to "copy" and "make derivative works" both sound in copyright—but to exercise those rights, it is necessary to exercise the patent right to "make." The right to "distribute" also implicates the right to sell, offer to sell, and import; to think otherwise would suggest that someone could avoid infringing a patent by giving away an otherwise-infringing item.

C. Implied Patent Licenses

As detailed above, every open source license written to be enforceable under U.S. law includes either a classical or an express patent grant. But open source licenses also may give rise to implied patent licenses.

The theory of implied patent licenses arises from *De Forest Radio Telephone Co. v. United States*. The classic statement establishing the theory of implied patent licensing is as follows:

> Any language used by the owner of the patent, or any conduct on his part exhibited to another from which that other may properly infer that the owner consents to his use of the patent in making or using it, or selling it, upon which the other acts, constitutes a license and a defense to an action for a tort.[36]

An implied license can be created by any communicative act by a patentee. It does not require specific words or phrases in an agreement. Rather, per *De Forest*, the focus of the implied license inquiry is on the language and actions of the patent owner or a licensee, and how the actions of the patent owner create expectations in the licensee.

Kappos and Harrington argue that "courts following precedent would be compelled to find against any implied patent license or any patent exhaustion theory in an OSD-compliant licensing context."[37] I disagree.

Kappos and Harrington focus their analysis on different theories that can ultimately give rise to an implied license, evaluating whether legal estoppel or equitable estoppel is more appropriate to the open source context (ultimately deciding that neither theory is

36. De Forest Radio Tel. Co. v. United States, 273 U.S. 236, 241 (1927).
37. Kappos & Harrington, *supra* note 2 (manuscript at 6).

appropriate).[38] Focusing on the label, however, misses the insight identified by the court in *Wang Labs., Inc. v. Mitsubishi Elecs. Am., Inc.*[39]:

> Since *De Forest*, this court and others have attempted to identify and isolate various avenues to an implied license. As a result, courts and commentators relate that implied licenses arise by acquiescence, by conduct, by equitable estoppel (estoppel in pais), or by legal estoppel. *These labels describe not different kinds of licenses, but rather different categories of conduct which lead to the same conclusion: an implied license.* The label denotes the rationale for reaching the legal result. . . .
>
> Neither this court nor the Supreme Court, however, has required a formal finding of equitable estoppel as a prerequisite to a legal conclusion of implied license.[40]

Per the *Wang* court, it is more important to look at the "conduct" of the licensor, and how it would be seen by a licensee. "The primary difference between the estoppel analysis in implied license cases and the analysis in equitable estoppel cases is that implied license looks for an affirmative grant of consent or permission to make, use, or sell: i.e., a license."[41] As noted above, even the briefest, most permissive open source licenses include at least an affirmative grant to "use" the software and the capability to "sell."[42] This is the exact conduct identified by the *Wang* court as leading to an implied patent license.

Even *Oracle v. Terix*,[43] which Kappos and Harrington use to support their argument, actually cuts the other way: "Courts have found implied licenses only in narrow circumstances where *one party created a work* at [the other's] request *and handed it over, intending that [the other] copy and distribute it.*"[44] In the case of open source, the work may not have been created "at the other's

38. *Id.* (manuscript at 5).

39. Wang Labs., Inc. v. Mitsubishi Elecs. Am., Inc., 103 F.3d 1571, 1583 (Fed. Cir. 1997).

40. *Id.* at 1580-81 (emphases added) (citations omitted).

41. *Id.* at 1581.

42. *See Licenses by Name*, *supra* note 35.

43. Oracle Am., Inc. v. Terix Comput. Co., Inc., No. 5:13-CV-03385 PSG, 2015 WL 2090191 (N.D. Cal. May 5, 2015).

44. *Id.* at *8 (quoting A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1026 (9th Cir. 2001)) (emphasis added).

request," but the act of releasing work under an open source license provides documented proof that the licensor "intend[ed] the other to copy and distribute it." The *Oracle* court rejected the defendants' argument that an implied license existed, because it didn't find that the plaintiff had acted in a way such that "[the] other [party] may properly infer that the owner consents to [its] use" of the work.[45] But in the case of OSS, releasing code under an open source license provides exactly that inference.[46]

IV. PATENT RIGHTS IN THE OPEN SOURCE DEFINITION

Based on the review above, essentially every open source license includes either a classic patent grant or an express patent grant, and the context also provides support for a court to find an implied patent license. This analysis is based on the text of the open source licenses themselves—which is what a court would primarily examine if trying to determine whether the licenses granted any patent rights.[47]

However, certain aspects of the OSD are helpful in evaluating what rights were intended to be included in all open source licenses. Given the weight that Kappos and Harrington appear to place on the OSD and other mailing list discussions, I will briefly address their points and make a few of my own.

A. The Open Source Definition is Deliberately Broad

The first argument advanced by Kappos and Harrington is that the OSD does not address patent rights. To the extent that this point is limited to the explicit statement that "nowhere in the OSD does it

45. *Id.* (quoting Field v. Google, 412 F.Supp.2d 1106, 1116 (D. Nev. 2006)).

46. Kappos and Harrington further assert in a footnote that "an OSS license that conveys no patent rights involves neither the selling of a product nor the licensing of a patent and does not implicate patent exhaustion." Kappos & Harrington, *supra* note 2 (manuscript at 6 n.14). However, this disregards *LifeScan Scot., Ltd. v. Shasta Techs., LLC*:: "[A] patentee cannot evade patent exhaustion principles by choosing to give the article away rather than charging a particular price for it. Where a patentee unconditionally parts with ownership of an article, it cannot later complain that the approach that it chose results in an inadequate reward and that therefore ordinary principles of patent exhaustion should not apply." 734 F.3d 1361, 1375 (Fed. Cir. 2013) (citations omitted). A transfer of software according to a license, regardless of the price charged for that license, *is* a transfer that implicates patent exhaustion.

47. *See, e.g.*, XimpleWare, Inc. v. Versata Software, Inc., 2014 U.S. Dist. LEXIS 68515, at * 15-16 (N.D. Cal. May 16, 2014) (evaluating the scope of the GPLv2 license based solely on its text, rather than on the Open Source Definition or other parol evidence).

state that an OSD-compliant license also conveys a patent grant," this is true.[48] The word "patent" does not appear in the text of the OSD.

However, this observation is less conclusive than it seems. For example, Kappos and Harrington agree that the OSD implicates copyright,[49] but the word "copyright" does not exist in the OSD either. It is inconsistent to assume that the OSD only implicates copyright, but not patents, when the text of the OSD is actually silent as to both terms.

Rather than focus on "patents" or "copyrights," the OSD instead focuses on the broad permissions required to be considered open source. For example, OSD 1 states that open source licenses "shall not restrict any party from selling or giving away the software. . . . The license shall not require a royalty or other fee for such sale."[50] Kappos and Harrington focus narrowly on the text stating that "the license shall not require a royalty" and miss the broader context: The specific right protected is the right of any party to *sell* the software, royalty-free. The right to sell is one of the core reserved rights under patent law.[51] All open source licenses comply with the OSD, by definition, and all open source licenses, therefore, incorporate this right.

In similar fashion, OSD 6 includes a right to use: "The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research."[52] Although this element is stated in the negative, the intention is clear: OSS programs may be *used* by any person for any purpose.

---

48. Kappos & Harrington, *supra* note 2 (manuscript at 3).

49. *Id.* ("There is no doubt that OSD-compliant licenses were designed to cover copyright and by extension, copyright royalties are not permitted.").

50. *The Open Source Definition (Annotated)*, *supra* note 8.

51. 35 U.S.C. § 271(a) (2000) ("[W]hoever without authority . . . offers to sell, or sells any patented invention . . . infringes the patent."). The copyright statute also mentions sale, but only in the context of the broader right to distribute copies. 17 U.S.C. § 106(3) (2010) ("The owner of copyright under this title has the exclusive rights . . . 3. to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending."). In copyright licenses, this is usually called the right to "distribute," whereas in patent licenses, the key word for this right is to "sell" or "offer to sell."

52. *The Open Source Definition (Annotated)*, *supra* note 8.

B. The Actions of the OSI Show That Patent Rights Cannot Be Excluded from Open Source Licenses

Kappos and Harrington note that they reviewed "all OSI License Discuss and License Review archives" for discussions relevant to patent rights and the OSD.[53] They highlight two mailing list threads in particular as informative: (1) an April 2009 thread on license-review,[54] and (2) a March 2017 thread on license-discuss.[55] Based on these mailing list discussions, they argue that the community showed a lack of "consensus" regarding the interaction of the OSD and patent rights.[56]

More significant than the mailing list discussions, however, are the actions of the OSI in the contexts identified in those discussions. In the April 2009 thread, the MPEG Working Group—a standard development organization interested in maintaining FRAND patent licensing—asks for OSI's approval of the "MXM Public License," which is an open source license modified particularly to allow licensors in the standard-setting group "to ask for a [patent] license separately from the copyright."[57] The request to certify the MXM License as open source was denied by the OSI.

Similarly, the March 2017 discussion arose from OSI's refusal to certify the "Creative Commons Zero" (CC0) license as open source. Again, the problem was an explicit reservation of patent rights. The OSI explained:

> The most serious of the concerns raised had to do with the effects of clause 4(a), which reads:
>
> *"No ... patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document."* While many open source licenses simply do not mention patents, it is exceedingly rare for open source licenses to explicitly disclaim any conveyance of patent rights, and the Committee felt that approving such a license

53. Kappos & Harrington, *supra* note 2 (manuscript at 3-4).

54. *See April 2009 Archives by thread*, OSI LICENSE-REVIEW ARCHIVES, http://lists.opensource.org/pipermail/license-review_lists.opensource.org/2009-April/thread.html ("For approval: MXM Public license" thread).

55. *See March 2017 Archives by thread,* OSI LICENSE-DISCUSS ARCHIVES, http://lists.opensource.org/pipermail/license-discuss_lists.opensource.org/2017-March/thread.html ("Patent rights and the OSD" thread).

56. Kappos & Harrington, *supra* note 2 (manuscript at 3).

57. *See For approval: MXM Public license*, OSI LICENSE-REVIEW ARCHIVES (Apr. 8, 2009), http://lists.opensource.org/pipermail/license-review_lists.opensource.org/2009-April/000716.html.

> would set a dangerous precedent, and possibly even weaken patent infringement defenses available to users of software released under CC0.[58]

C. The Author of the Open Source Definition Meant it to Cover Patent Rights

Kappos and Harrington's review appears to have missed a significant response to the April 2009 thread they highlight. The message was posted by Bruce Perens, one of the directors and original members of the OSI. It is significant enough that it deserves to be quoted at length:

> I am the creator of the Open Source Definition, and thus can shed some light on the parts that might be seen as ambiguous . . . .
>
> The OSD does not distinguish between copyright, moral rights, patents, contract restriction, or any other means of restricting what someone can do with software. It applies equally to all of those. And thus I believe that your proposed license, by making explicit that patent rights are not granted for a large class of binary derivatives of the program, violates most of the OSD rules, not just rule number 7.
>
> You could, however, construct a license that is . . . sufficiently restrictive that many implementors would prefer to license commercially. You can simultaneously place your reference implementation under a commercial license and an Open Source license like AGPL3, so that those who wish to commercially license the patents have a well-defined path for doing so . . . .
>
> . . . .
>
> So, what you get is the "free" world using the patent without charge, and the proprietary world using it under license and paying royalties.
>
> This is not perfect . . . . But it's the best I can offer you if you want to be OSD compliant.[59]

---

58. *See Frequently Answered Questions*, OPEN SOURCE INITIATIVE, https://opensource.org/faq#cc-zero (last visited Apr. 24, 2019).

59. *See* Bruce Perens, *What would work instead of the MXM public license?*, OSI LICENSE-REVIEW ARCHIVES (Apr. 14, 2009),

Thus, in contrast to Kappos and Harrington's findings, the author of the Open Source Definition specifically and definitively addressed the issue: a royalty-free patent grant is necessary for compliance with the OSD.

V. OSS AND FRAND ARE COMPLEMENTARY, NOT COMPATIBLE

Turning to the "bigger picture," Kappos and Harrington argue that trying to respect the royalty-free status of OSS results in a kind of "forced license" when open source code is used in the context of a standard.[60] This argument fundamentally misses the point that FRAND-based standard setting and OSS are two *different* types of innovation development regimes with *different* standards. They can be used alongside each other. But a patent holder cannot apply FRAND-style royalties to code while simultaneously distributing that same code under an open source. The requirements of the two licensing regimes—FRAND and open source—are complementary, not compatible.

As noted above, Kappos, Harrington, and I all agree that the FRAND-based standard-setting process has resulted in remarkable innovation and development.[61] This process has a history and rules that must be respected for the process to work. Among these rules are the intellectual property rights policies of various organizations—policies that allow for and expect the imposition of FRAND-based royalties.

We also agree that the collaborative production of open source communities has resulted in remarkable innovation and development. Like the traditional standard-setting process, it also has a history and rules—including the licensing of intellectual property on a royalty-free basis for the purposes of collaborative development. In fact, it is the free, messy, noisy collaboration of many different parties with different interests that has resulted in the innovative development that Kappos and Harrington admire.[62] Open source has a much shorter organized history than traditional standards processes, but it has "come out of nowhere" within a relatively short time to dominate all other software development

---

http://lists.opensource.org/pipermail/license-review_lists.opensource.org/2009-April/000757.html.

60. Kappos & Harrington, *supra* note 2 (manuscript at 7).

61. *See* sources cited *supra* note 6.

62. *See generally* Eric S. Raymond, *The Cathedral and the Bazaar* (2000), http://www.catb.org/esr/writings/cathedral-bazaar/cathedral-bazaar/.

methodologies. A recent estimate stated that 98% of all businesses use open source code in their products or operations.[63]

The problem, however, is that the policy solution advocated by Kappos and Harrington privileges FRAND-based standard-setting to the detriment of open source. They argue that when standard-setting communities intentionally incorporate OSS-licensed code into a standard, it is the royalty-free status of open source that should give way, *not* the payment of the FRAND-based royalty.

If adopted, however, their policy would have the effect of turning the royalty-free OSS world, with its attendant innovation, into a mere adjunct of the FRAND-based royalty-bearing world. In doing so, they would break the promise that OSS licensees could take any action allowed by the OSS license without requiring the "execution of an additional license [between licensor and licensee]."[64] Not to lean too heavily on a cliché, but this would have the effect of killing the goose that laid the golden eggs.

This is why open source and FRAND are *complementary*, not *compatible*: they rely on different intellectual property policies to generate innovation. These two development models can learn from each other, and compete with each other, but they are based upon fundamentally different underlying principles.

It is understandable why standard-setting organizations want to incorporate OSS: open source is inexpensive, interoperable, and innovative. Standard-setting organizations have the ability to change to become interoperable with OSS: simply adopt a royalty-free IPR policy, as many organizations have done. But those standard-setting organizations that wish to charge FRAND royalties ultimately have the same option that commercial enterprises have when dealing with open source: respect the licenses and rules that govern the usage of OSS, or take the time to create a commercial version that doesn't have the same licensing cost.

---

63. Ido Benmoshe, *Open source adoption: Risk factors for the enterprise*, ZEND (Mar. 15, 2017) https://blog.zend.com/2017/03/15/open-source-adoption-risk-factors-for-the-enterprise/.

64. *The Open Source Definition (Annotated)*, *supra* note 8.

Chapter 22

Defensive Patent Playbook (James M. Rice)

THE DEFENSIVE PATENT PLAYBOOK

James M. Rice†

Billionaire entrepreneur Naveen Jain wrote that "[s]uccess doesn't necessarily come from breakthrough innovation but from flawless execution. A great strategy alone won't win a game or a battle; the win comes from basic blocking and tackling."[1] Companies with innovative ideas must execute patent strategies effectively to navigate the current patent landscape. But in order to develop a defensive strategy, practitioners must appreciate the development of the defensive patent playbook.

Article 1, Section 8, Clause 8 of the U.S. Constitution grants Congress the power to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[2] Congress attempts to promote technological progress by granting patent rights to inventors. Under the utilitarian theory of patent law, patent rights create economic incentives for inventors by providing exclusivity in exchange for public disclosure of technology.[3] The exclusive right to make, use, import, and sell a technology incentivizes innovation by enabling inventors to recoup the costs of development and secure profits in the market.[4]

Despite the conventional theory, in the 1980s and early 1990s, numerous technology companies viewed patents as unnecessary and chose not to file for patents.[5] In 1990, Microsoft had seven utility patents.[6] Cisco

† J.D. Candidate, 2016, University of California, Berkeley, School of Law.

1. Naveen Jain, *10 Secrets of Becoming a Successful Entrepreneur*, INC. (Aug. 13, 2012), http://www.inc.com/naveen-jain/10-secrets-of-becoming-a-successful-entrepreneur.html.

2. U.S. CONST. art. 1 § 8, cl. 8.

3. *See* Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265, 266 (1977).

4. *See* Mark A. Lemley, *Ex Ante Versus Ex Post Justifications for Intellectual Property*, 71 U. CHI. L. REV. 129, 129–30 (2004).

5. *See* Colleen V. Chien, *From Arms Race to Marketplace: The Complex Patent Ecosystem and Its Implications for the Patent System*, 62 HASTINGS L.J. 297, 302–03 (2010) [hereinafter Chien, *From Arms Race to Marketplace*].

filed for one patent between 1984 and 1993.[7] Oracle opposed software patents at the United States Patent and Trademark Office ("PTO") hearings in 1994.[8] While these companies were not representative of the entire market, companies did not file patents to the extent seen today.[9]

Multiple factors in the patent landscape caused a dramatic shift in the use of the patent system. First, the Federal Circuit situated the patent system for rapid growth through significant reversals of patent denials by the PTO.[10] With the patent system primed for growth, Texas Instruments ("TI") and International Business Machines ("IBM") catalyzed a patent aggregation "arms race" that increased patent filings industry-wide.[11] As a result, webs of fragmented and overlapping patent rights, called patent thickets, developed in many innovative areas.[12]

After the dot-com bubble collapsed, non-practicing entities ("NPEs") emerged on the patent playing field.[13] Patent thickets and aggressive litigation by non-practicing entities turned the patent system on its head.[14] As a result, companies developed an array of defensive options and strategies to counter the changing use of patents. However, the tactics

6. This number resulted from a search for "Microsoft" as assignee on the U.S. Patent & Trademark Office's website. *See* Patent Full-Text and Image Database, http://patft.uspto.gov (last visited Nov. 19, 2014).

7. *Competition and Intellectual Property Law and Policy in the Knowledge-Based Economy: Joint Hearings Before the Fed. Trade Comm'n & Dep't of Justice* 673–74 (Feb. 28, 2002) (statement of Robert Barr, Vice President for Intellectual Property and Worldwide Patent Counsel, Cisco Systems, Inc.), *available at* http://www.ftc.gov/sites/default/files/documents/public_events/competition-ip-law-policy-knowledge-based-economy-hearings/020228ftc.pdf.

8. *Public Hearing on Use of the Patent System to Protect Software-Related Inventions: Before Bruce A. Lehman, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks*, USPTO 140 (1994) (statement of Jerry Baker, Senior Vice President, Oracle Corp.) ("I cannot find any evidence that patents for software will tend to [promote technological progress]. Indeed, every indication is to the contrary."), *available at* http://www.uspto.gov/web/offices/com/hearings/software/sanjose/sjhrng.pdf.

9. According to the U.S. Patent and Trademark Office ("PTO"), there were 176,264 patent filings in 1990, compared to 609,052 in 2013. PATENT TECHNOLOGY MONITORING TEAM, U.S. PATENT & TRADEMARK OFFICE, U.S. PATENT AND STATISTICS CHART, CALENDAR YEARS 1963–2013 (2014), *available at* http://www.uspto.gov/web/offices/ac/ido/oeip/taf/us_stat.htm.

10. Arti K. Rai, *Who's Afraid of the Federal Circuit?*, 121 YALE L.J. ONLINE 335, 338 (2011), http://www.yalelawjournal.org/forum/whos-afraid-of-the-federal-circuit.

11. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 304.

12. Carl Shapiro, *Navigating the Patent Thicket: Cross Licensing, Patent Pools, and Standard Setting* in INNOVATION POLICY AND THE ECONOMY 119, 119–20 (Adam B. Jaffe et al., eds., 2001).

13. *See infra* Part II.

14. *See id.*

needed to navigate the patent system evolved as the landscape shifted. The analysis below follows the chronological evolution of defensive strategies and sets forth a defensive patent playbook for practitioners in the patent field.

This Note proceeds in four parts. Each Part reviews the development of the patent landscape as a necessary backdrop for an analysis of various defensive patent plays. The issues from each era cumulated to shape the current patent landscape. Part I evaluates early defensive methods used to navigate webs of overlapping patent rights. Part II describes the rise of NPEs, changes in substantive doctrines, and additional strategies introduced in the wake of the dot-com bubble. Part III discusses the current trend towards increased monetization, and assesses defensive options in the current landscape. Part IV explores defensive tactics that may become widely used in the future.

I. EARLY HISTORY

Many technology companies did not seek patent rights on their innovations in the 1980s and early 1990s.[15] However, the emergence of computer platform-based technologies transformed the patent system. This Part traces the development of the patent landscape during the mid- to late-1990s and analyzes the defensive strategies developed during this era to combat the changing use of patents.

A. BACKGROUND: THE DEVELOPMENT OF PATENT THICKETS

During the "early history," companies shifted their use of patents after actions by the Federal Circuit prompted growth in the patent system.[16] In the 1980s and 1990s the Federal Circuit expanded patent law in the areas of computer software and biotechnology by repeatedly reversing PTO patent denials.[17] Further, through a series of decisions, the Federal Circuit relaxed the requirement that inventions be a nonobvious improvement over the prior art.[18] Scholars contend that these changes "pushed the law

15. *See* Chien, *From Arms Race to Marketplace*, *supra* note 5, at 302–03.

16. Rai, *supra* note 10, at 338.

17. *Id.*

18. Robert Hunt, *Patent Reform: A Mixed Blessing for the U.S. Economy*, FED. RESERVE BANK OF PHILA. BUS. REV. 15, 20–21 (Nov./Dec. 1999), *available at* http://www.philadelphiafed.org/research-and-data/publications/business-review/1999/november-december/brnd99rh.pdf.

in an excessively pro-patent direction, broadening the scope of patentable matter and endowing patentees with unwarranted power."[19]

With the patent system situated for growth, TI and IBM stimulated a patent "arms race" that increased patenting industry-wide.[20] When facing bankruptcy in the mid-1980s, TI initiated a licensing and litigation campaign to save the company.[21] At first, TI took an adversarial stance, but it gradually shifted towards a licensing model.[22] By the 2000s, TI had accumulated an expansive patent portfolio and an estimated four billion dollars in licensing fees.[23] Around the same time, IBM started a licensing and assertion campaign.[24] Armed with a quarter of the software patents granted by the PTO between 1978 and 1988, IBM's campaign brought in millions of dollars in licensing revenue.[25]

By the 1990s, practicing companies grew tired of paying licensing fees and filed more patent applications under the newly relaxed patenting standard.[26] Companies developed larger patent portfolios because of their shifting views on the importance of acquiring patents for defensive purposes rather than increased research and development spending.[27] As a result, private parties increasingly held exclusive rights in prior discoveries, and patent thickets began to develop in key industries such as biotechnology and computer software.[28] Because cumulative innovation occurs when an invention builds on prior discovers,[29] these patent thickets became an obstacle to future innovation.[30] Too many owners held exclusive patent rights that inventors sought to build upon.[31]

19. Jonathan Masur, *Patent Inflation*, 121 YALE L.J. 470, 477–78 (2011); *see* Donald R. Dunner et al., *A Statistical Look at the Federal Circuit's Patent Decisions: 1982–1994*, 5 FED. CIR. B.J. 151, 151 (1995).

20. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 304.

21. *Id.*

22. *Id.* at 305.

23. *Id.* at 304.

24. *Id.* at 305.

25. *Id.* at 304–06.

26. *Id.* at 306.

27. *Id.*

28. Shapiro, *supra* note 12, at 119.

29. *Id.* at 119–20 (noting Sir Isaac Newton's statement that each scientist "stands on the shoulders of giants" to reach new heights).

30. Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCI. 698, 698 (1998).

31. *Id.*

Furthermore, excessive privatization occurred in developing platform technologies with significant network externalities.[32] These technologies needed standards for maximum user benefit.[33] In industries such as computer software and telecommunications, formal standard setting was "a core part of bringing new technologies to market."[34] Excessive patent rights threatened to prevent the development of these standards and to impose a "drag on innovation and commercialization of new technologies."[35]

Excessive privatization amplified three key transaction costs that companies had to overcome in order to assemble patent rights—search costs, holdouts, and licensing costs.[36] First, the search costs of a patent transaction were costly due to the intangible nature of patent rights.[37] Unlike tangible property that can be clearly defined, the boundaries of patent rights generally remain blurred until a federal court interprets the patent's claims.[38] A thicket of patents with unclear boundaries placed inventors in a costly struggle to determine where there was freedom to operate and which patents were relevant to their efforts.[39]

---

32. *See generally* Peter S. Menell, *Tailoring Legal Protection for Computer Software*, 39 STAN. L. REV. 1329 (1987):

> Network externalities exist in markets for products for which the utility or satisfaction that a consumer derives from the product increases with *the number of other consumers of the product*. The telephone is a classic example of a product for which there are network externalities. The benefits to a person from owning a telephone are a function of the number of other people owning telephones connected to the same telephone network . . .

Id. at 1340 (emphasis added).

33. *See* James C. De Vellis, *Patenting Industry Standards: Balancing the Rights of Patent Holders with the Need for Industry-Wide Standards*, 31 AIPLA Q.J. 301, 303 (2003) ("Industry standards are critical in an increasingly interdependent, technology-based world.").

34. Shapiro, *supra* note 12, at 119.

35. *See id.* at 121–24; *see also* Heller & Eisenberg, *supra* note 30, at 698–99 (describing the "tragedy of the anticommons" that can occur with the proliferation of intellectual property rights).

36. *See* Justin R. Orr, Note, *Patent Aggregation: Models, Harms, and the Limited Role of Antitrust*, 28 BERKELEY TECH. L.J. 525, 531–32 (2013).

37. Peter S. Menell & Michael J. Meurer, *Notice Failure and Notice Externalities*, 5 J. LEGAL ANALYSIS 1, 2 (2013).

38. Orr, *supra* note 36, at 529 n.22. Federal courts interpret the meaning of a patent's claims, which clarify the boundaries of the patent right, in hearings referred to as "Markman" hearings. *Id.; see also* Markman v. Westview Instruments, Inc., 517 U.S. 370 (1996).

39. *See* Menell & Meurer, *supra* note 37, at 1–2.

Second, companies faced holdout problems, which occur when a patent holder learns that its patent rights are essential to an inventor's overall plan.[40] As the inventor reaches licensing agreements with more patent holders, the inventor becomes more committed to the project, and the remaining patent holders gain leverage to demand a higher fee.[41] Patent thickets exacerbated this problem because an inventor must purchase rights from numerous patent holders to make, use, or sell a new invention that builds upon prior patents.[42]

Finally, negotiating individual licensing agreements with a large number of companies in the industry became prohibitively expensive.[43] In industries where a single product may relate to hundreds of patents, companies avoided attempting to overcome the patent thicket through negotiated licenses and refrained from introducing new products.[44] For instance, according to one commentator, a large company in the pharmaceutical industry developed a treatment for Alzheimer's disease, but it did not release the drug due to the threat of overwhelming litigation.[45]

Companies needed to develop strategies to overcome the costs associated with fragmented patent rights, especially in the computer software, telecommunications, and biotechnology industries.[46] Consequently, defensive plays materialized to combat excessive privatization.

B. DEFENSIVE PLAYS IN THE EARLY HISTORY

During this era, companies developed three major strategies to navigate the patent thicket: (1) defensive patent aggregation, (2) standard setting and RAND cross-licensing and (3) open source software. These strategies make up the first group of "plays" in the defensive patent playbook.

---

40. Michael Mattioli, *Power and Governance in Patent Pools*, 27 HARV. J.L. & TECH. 421, 428 (2014).

41. *Id.*

42. *See* Mark A. Lemley, *Ten Things to Do About Patent Holdup of Standards (and One* Not *to)*, 48 B.C. L. REV. 149, 150–52 (2007).

43. *See* Jason Schultz & Jennifer M. Urban, *Protecting Open Innovation: The Defensive Patent License as a New Approach to Patent Threats, Transaction Costs, and Tactical Disarmament*, 26 HARV. J.L. & TECH. 1, 8 (2012).

44. Shapiro, *supra* note 12, at 126.

45. MICHAEL HELLER, THE GRIDLOCK ECONOMY: HOW TOO MUCH OWNERSHIP WRECKS MARKETS, STOPS INNOVATION, AND COSTS LIVES 4–5 (2008).

46. *See* Shapiro, *supra* note 12, at 119.

1. Defensive Patent Aggregation

Companies began to use the defensive aggregation play industry-wide in the late 1990s.[47] The cost of paying for patent licenses, like those paid to TI and IBM, and the lack of freedom to operate spurred the growth of patent aggregation as a defensive strategy.[48] Companies aggregated patents to deter lawsuits, rather than to assert offensively.[49]

Defensive patent portfolios offer no legal defense but can be used to bring counterclaims in a patent suit.[50] Colleen Chien compared mass patent aggregation to the nuclear arms race with each company viewing its patents as instruments of mutually assured destruction.[51] For example, suppose that Company *X* claims that Company *Y* infringes its patents. If Company *Y* has an extensive patent portfolio that potentially covers Company *X*'s products, Company *Y* will likely counter with an assertion of patent infringement against Company *X*. The threat of countersuit creates an incentive for the companies to enter into a cross-licensing agreement or drop their suits.[52]

The size and scope of the patent portfolio dictate the effectiveness of the strategy.[53] During cross-licensing negotiations, the parties rarely scrutinize each individual patent.[54] Companies instead focus on quantity rather than quality because of the high cost of determining the validity and scope of each patent claim.[55] As a result, the aggregated patent portfolio provides "a stronger patent position than the sum of its patent parts."[56] However, defensive aggregation requires symmetrical risks to deter litigation.[57] As discussed in Part II, NPEs do not face the same retaliatory

47. *See* Chien, *From Arms Race to Marketplace*, *supra* note 5, at 304–308 (noting that defensive patent strategies date back to at least the beginning of the twentieth century when Henry Ford aggregated automobile patents to reduce the risk of being sued and ensure freedom to operate).

48. *Id.* at 304.

49. Schultz & Urban, *supra* note 43, at 6.

50. *See id.*

51. Chien, *From Arms Race to Marketplace, supra* note 5, at 334; *see generally* Henry S. Rowen, *Introduction*, in GETTING MAD: NUCLEAR MUTUAL ASSURED DESTRUCTION, ITS ORIGINS AND PRACTICE 1–13 (Henry D. Sokolski, ed., 2004).

52. Schultz & Urban, *supra* note 43, at 6–7.

53. *Id.* at 6.

54. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 308.

55. *Id.*

56. Orr, *supra* note 36, at 526.

57. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 317.

risks because they do not make, use, import, or sell any infringing product.[58]

Defensive aggregation allows companies to combat excessive privatization by creating a "patent stalemate" with other practicing companies.[59] In addition to defensive aggregation, another play developed in the early history to assist the assimilation of patent rights in platform-based technologies.

2. Standard Setting/RAND Cross-Licensing

Standard setting and reasonable and nondiscriminatory ("RAND") licensing pledges provide companies with a method for overcoming transaction costs and standardization issues. Standard-setting organizations ("SSOs") set standards to promote coordination and interoperability.[60] When SSOs incorporate patented technology into a standard, the patent holder gains leverage and the power to holdout for inflated licensing rates because of the expense of switching to a different standard.[61] SSOs attempt to "mitigate the tension between proprietary rights and the need for interoperability" through RAND pledges.[62]

A RAND pledge is a commitment to offer implementers of a standard a reasonable license to any patents necessary to implement the standard.[63] Prior to incorporation into a standard, SSOs require patent holders to disclose all patents or pending patent applications relevant to the standard and to submit a Letter of Assurance.[64] In the Letter of Assurance, patent

58. *See infra* Part II.

59. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 317.

60. Marc Rysman & Timothy Simcoe, *Patents and the Performance of Voluntary Standard-Setting Organizations,* 54 MGMT. SCI. 1920, 1922–23 (2008).

61. *See* U.S. DEP'T OF JUSTICE & USPTO, POLICY STATEMENT ON REMEDIES FOR STANDARDS-ESSENTIAL PATENTS SUBJECT TO VOLUNTARY F/RAND COMMITMENTS 1 n.2 (2013), *available at* http://www.uspto.gov/about/offices/ogc/Final_DOJ-PTO_Policy_Statement_on_FRAND_SEPs_1-8-13.pdf.

62. Kassandra Maldonado, Note, *Breaching RAND and Reaching for Reasonable:* Microsoft v. Motorola *and Standard-Essential Patent Litigation*, 29 BERKELEY TECH. L.J. 419, 422 (2014).

63. Jorge L. Contreras & Richard J. Gilbert, *A United Framework for RAND and Other Reasonable Royalties*, 30 BERKELEY TECH. L.J. (forthcoming 2015) (manuscript at 4), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2502066.

64. *See, e.g.*, INT'L ELECTROTECHNICAL COMM'N ET AL, GUIDELINES FOR IMPLEMENTATION OF THE COMMON PATENT POLICY 15 (providing a General Patent Statement and Licensing Declaration Form For ITU-T or ITU-R Recommendation) *available at* http://www.itu.int/dms_pub/itu-t/oth/04/04/T04040000010003PDFE.pdf (last visited Jan. 16, 2015); *Letter of Assurance for Essential Patent Claims*, IEEE,

holders agree to license their patents on RAND terms if their patent becomes essential to the practice of the standard.[65] If patent holders decline to make RAND commitments, their technology will not be integrated into the standard.[66]

Companies throughout the technology industry implement standards in order to compete in the market and provide interoperable products. In theory, implementers of the standard gain access to patented technology at a reasonable rate, and patent holders benefit through the widespread adoption of their technology and reasonable royalty rights. The patents encumbered by a RAND commitment may still be licensed and asserted, but the patent holder must offer the implementer reasonable licensing terms.[67] However, after seeking RAND commitments, SSOs rarely become involved in the licensing process.[68]

This lack of oversight allows standard essential patent ("SEP") holders to utilize RAND-encumbered patents as offensive and defensive weapons, to encourage cross-licensing.[69] If a company asserts patent infringement of a non-SEP patent, the alleged infringer can utilize their RAND-encumbered SEPs in the same manner as other patents are utilized.[70] If a party implements the standard, they necessarily infringe the SEP. Thus, the threat of mutually assured destruction can reduce litigation and forcibly encourage cross-licensing agreements.[71] However, a recent court ruling has modified patent holders' ability to obtain injunctions on

http://standards.ieee.org/about/sasb/patcom/loa-802_11-kpn-08Jan2013.pdf (last visited Jan. 16, 2015).

65. Contreras & Gilbert, *supra* note 63, at 1–2.

66. *See, e.g.*, Int'l Telecomm. Union, *Common Patent Policy for ITU-T/ITU-R/ISO/IEC*, http://www.itu.int/en/ITU-T/ipr/Pages/policy.aspx (last visited Jan. 16, 2015).

67. *See, e.g.*, *Letter of Assurance for Essential Patent Claims*, *supra* note 64.

68. Jay P. Kesan & Carol M. Hayes, *FRAND's Forever: Standards, Patent Transfers, and Licensing Commitments*, 89 IND. L.J. 231, 239 (2014).

69. *See generally* Thomas H. Chia, Note, *Fighting the Smartphone Patent War with RAND-Encumbered Patents*, 27 BERKELEY TECH. L.J. 209, 209–11 (2012) (defining standard essential patents as patents that are necessary to implement a given standard); Shapiro, *supra* note 12, at 119–120 (describing the "risk of holdup").

70. *See* Dan O'Connor, *Standard-Essential Patents in Context: Just a Small Piece of the Smartphone War Puzzle*, PATENT PROGRESS (Mar. 5, 2013), http://www.patentprogress.org/2013/03/05/standard-essential-patents-in-context-just-a-small-piece-of-the-smartphone-war-puzzle/.

71. Chia, *supra* note 69, at 213–14.

RAND-encumbered patents.[72] Part III evaluates this modification and the play's role in the current patent landscape.[73]

In conclusion, standard setting and RAND pledges enable companies to provide interoperable products in platform-based technologies.[74] Patent holders benefit from the adoption of their technology, and implementers acquire patented technology at a reasonable rate. But the breach of RAND pledges limits the effectiveness of the play.

3. Open Source Software

In addition to RAND pledges, open source software emerged as an alternative approach to software development.[75] The label "open source" refers to the distribution of source code used to develop software programs so that other programmers can study and modify the code.[76] The success of open source depends on shared contributions to a nonproprietary model and the theory that the motivations to innovate go beyond the economic incentives achieved through exclusivity.[77]

Open source software originated with Richard Stallman's operating system, which he called GNU.[78] Stallman granted individuals a license to modify his source code and distribute it to others under the GNU General Public License ("GPL").[79] But Stallman required the person who modified and distributed the software to grant others the same conditions granted under the GPL.[80] Open source software progressed when Linus Torvalds built upon Stallman's foundation and shared his kernel, a central component of the operating system, under the GPL.[81] Torvalds's kernel became known as Linux.[82]

72. *See* Apple, Inc. v. Motorola, Inc., 757 F.3d 1286, 1331–32 (Fed. Cir. 2014).
73. *See infra* Part III.
74. *See* Rysman & Simcoe, *supra* note 60, at 1922–23.
75. YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 63–67 (2006).
76. *See* Sara Boettinger & Dan L. Burk, *Open Source Patenting*, 1 J. INT'L BIOTECHNOLOGY L. 221, 222 (2004) (defining "open source" and explaining that programmers typically use programming languages, the source code, to develop software that is then translated to a machine-readable format, called object code, which programmers cannot understand or analyze when distributed).
77. *See* BENKLER, *supra* note 75, at 94–99.
78. *Id.* at 64.
79. *Id.* at 65.
80. *Id.*
81. *Id.* at 65–66.
82. *Id.*

After a decade of incremental improvements, technology companies in mainstream industry began to utilize open source software.[83] This utilization promotes innovation and limits the enforcement of patents that use open source software.

a) Open Source License Benefits

Open source licenses promote innovation by increasing competition and empowering diverse problem solving. Open source increases competition by acting as a "valuable check on potential monopoly power."[84] Enhanced competitiveness yields lower prices and accelerates innovation.[85] For example, in 1998, a leaked internal memorandum from Microsoft revealed that a Microsoft strategist considered open source software a major threat to the company's dominance over the desktop computer.[86] The increased competition generated through open source licenses prohibited Microsoft from monopolizing the desktop operating platform and charging inflated prices.[87]

Further, open source licenses spur technological development by enabling numerous programmers to contribute to open source projects.[88] The presence of a wide range of contributing licensees allows society to benefit from a multitude of diverse approaches to solving technological issues.[89] Resulting technological developments benefit consumers and companies seeking to promote innovation to achieve business objectives.

b) Open Source Limits on Patent Rights

Using software subject to an open source license does not affect the ability to *obtain* patent protection, but it severely curtails the *enforcement* of patent rights.[90] If a programmer includes software under an open source

83. *Id.* at 66.

84. James Boyle, *Open Source Innovation, Patent Injunctions, and the Public Interest*, 11 DUKE L. & TECH. REV. 30, 31–32 (2012) (noting that, although most prevalent in computer software, open source licensing can be "found in areas ranging from synthetic biology to the development of artificial limbs.").

85. *Id.*

86. BENKLER, *supra* note 75, at 123.

87. *See* Robert P. Merges, *A New Dynamism in the Public Domain*, 71 U. CHI. L. REV. 183, 193 (2004).

88. FED. TRADE COMM'N., THE EVOLVING IP MARKETPLACE: ALIGNING PATENT NOTICE AND REMEDIES WITH COMPETITION (Mar. 2011), *available at* http://www.ftc.gov/reports/evolving-ip-marketplace-aligning-patent-notice-remedies-competition.

89. Boyle, *supra* note 84, at 32.

90. *See id.*

licensing agreement in a proprietary program, the patent holder limits the enforceability of its patent rights against downstream users.

First, under the GPL Agreement, contributors grant the licensee—any user of the open source software—a copyright license to their software.[91] In addition to the direct license granted, companies may be prohibited from utilizing patent rights they have *licensed from third parties* in open source projects.[92] For instance, Company A receives a patent license from a third party for GreatSoftware with no right to sublicense GreatSoftware. Company A wants to utilize GreatSoftware in an open source project under the GPL. However, because Company A does not have the ability to sublicense GreatSoftware, it cannot satisfy the licensing requirements of the GPL. Thus, Company A must either remove GreatSoftware from its product or not distribute the open source project containing GreatSoftware. Therefore, the requirements of the open source license limit Company A's ability to utilize patent rights licensed from a third party in conjunction with open source software.

Although open source licenses severely limit the direct use of patent rights, patent holders may still utilize their rights in certain situations. Under the GPL, even if patented technology contains open source software, patent holders may still (1) engage in licensing and assertion campaigns against infringers not using the inventor's open source code, (2) distribute a patented version of software without the open source code, and (3) assert patent rights against redistributors that do not conform to the open source license terms.[93] For example, if a competitor sells an infringing product not derived from the inventor's original code, the patent holder may assert its patent rights against the competitor because users who independently created other software are not granted a license.[94] Ironically, the patent holder will likely be unable to assert patent rights against competitors who copy its source code, but will be able to assert patent rights against competitors who did not copy the source code.[95]

91. GNU, GNU General Public License Version 1, GNU OPERATING SYSTEM (Feb. 1989), https://www.gnu.org/licenses/gpl-1.0.html.

92. Laura A. Majerus, *Patent Rights and Open Source—Can They Co-exist?*, FENWICK & WEST LLP INTELL. PROP. 2006 SUMMER BULL. 1, 2–3 (June 30, 2006), http://www.fenwick.com/FenwickDocuments/IP_Bulletin_Summer_2006.pdf.

93. *Id.*

94. *Id.*

95. Gene Quinn, *Beware Open Source Strings Attached if You Want a Patent*, IP WATCHDOG (Oct. 12, 2010), http://www.ipwatchdog.com/2010/10/12/beware-open-source-strings-attached-if-you-want-a-patent/id=12787/.

As software patents became more prevalent in the 2000s, open source licenses began to include reciprocal patent agreements, in addition to copyright provisions, to ensure that software patents could not prevent the use or modification of open source software.[96] Part III evaluates how these patent provisions altered this play and describes "infection" defenses provided by open source software.[97]

c) Summary of Open Source Licenses

Open source provides an alternative approach to innovation that enhances competitiveness and enables numerous programmers to contribute to open source projects. Although the first two versions of the GPL only granted a copyright license, the inclusion of open source software in proprietary programs limits patent holders' ability to enforce patent rights.

II. POST-DOT-COM BUBBLE

After the dot-com bubble burst, obstacles within the patent system accumulated. As practicing companies shifted their use of the patent system and patent thickets expanded, an influential player emerged on the patent playing field—the NPE. The term "NPE" generally refers to patent holders who monetize their patents without producing a product or practicing the technology.[98] The rise of the NPE (or "patent troll")[99] dramatically altered the patent landscape. This Part introduces a broad strategy to influence substantive doctrinal changes through lobbying and evaluates three additional plays that surfaced during this era: public disclosure, patent pledges, and RPX defensive protection.

A. BACKGROUND: RISE OF THE NPES

When the dot-com bubble collapsed, failed startup companies ("startups") provided NPEs with an abundance of patents. During the 1990s and 2000s, startups accumulated patents as tools to receive venture

96. Simon Phipps, *4 Ways Open Source Protects You Against Software Patents*, INFOWORLD (Nov. 8, 2013), http://www.infoworld.com/article/2609614/open-source-software/4-ways-open-source-protects-you-against-software-patents.html.

97. *See infra* Part III.

98. Orr, *supra* note 36, at 525 n.3.

99. "Patent troll" references the children's tale where three billy goats must pay a fee to the troll waiting under the bridge in order to pass. Robin Feldman & Tom Ewing, *The Giants Among Us*, 2012 STAN. TECH. L. REV. 1 (2012).

capitalist funding.[100] Startups that owned patents attracted larger investment amounts and experienced longer incubation periods.[101] In the early 2000s, the speculative bubble in the stock market quickly deflated, and "[w]hen the dot-coms came crashing down, many in the IP world suspected that the bankrupt companies held hidden treasures."[102] NPEs purchased such patent "treasures" at bankruptcy proceedings from failed startups and other technology companies.[103]

Alternative billing arrangements allowed NPEs to take advantage of asymmetrical costs.[104] In the past, attorneys generally billed clients in patent litigation on an hourly basis.[105] However, NPEs began utilizing the contingent-fee arrangement popularized by Jerome Lemelson and his attorney, Gerald Hosier.[106] A contingent-fee arrangement occurs when a lawyer represents a plaintiff in exchange for a specified percentage of the damages or settlement recovered from the defendant.[107] In patent cases, a defendant typically searches extensively for prior art in order to make an invalidity argument, which results in significant discovery costs.[108] NPEs take advantage of lower discovery costs and a contingent-fee arrangement as a strategic advantage against defendants using the more expensive hourly billing structure.[109]

While NPEs assert some legitimate claims of patent infringement, they predominately monetize patents with weak claims of infringement through "nuisance suits."[110] Although research shows that NPEs generally

100. Jerry X. Cao & Po-Hsuan Hsu, *The Informational Role of Patents in Venture Capital Financing* 1 (June 8, 2011), *available at* http://ssrn.com/abstract=1678809.

101. *Id.* at 23.

102. Lisa Lerer, *Going Once*, ALM IP L. & BUS., Oct. 2005, at 12.

103. Robin M. Davis, Note, *Failed Attempts to Dwarf the Patent Trolls: Permanent Injunctions in Patent Infringement Cases Under the Proposed Patent Reform Act of 2005 and* eBay v. MercExchange, 17 CORNELL J.L. & PUB. POL'Y 431, 431–32 (2008).

104. *See* James E. Bessen & Michael J. Meurer, *Essay: The Direct Costs from NPE Disputes*, 99 CORNELL L. REV. 387, 413 (2014).

105. David L. Schwartz, *The Rise of Contingent Fee Representation in Patent Litigation*, 64 ALA. L. REV. 335, 338 (2012).

106. *See* Chien, *From Arms Race to Marketplace*, *supra* note 5, at 311–12 (noting that Jerome Lemelson pioneered NPE licensing and assertion campaigns in the 1980s and 1990s by signing licenses with over a thousand companies and earning over a billion dollars).

107. Murray L. Schwartz & Daniel J. B. Mitchell, *An Economic Analysis of the Contingent Fee in Personal-Injury Litigation*, 22 STAN. L. REV. 1125, 1125 (1970).

108. *See* Schwartz, *supra* note 105, at 349–53.

109. *See* Bessen & Meurer, *supra* note 104, at 413.

110. "Nuisance suits" refer to instances when a patent owner files a patent infringement claim "seeking to license even clearly bad patents for royalty payments small

lose in summary judgment or during trial,[111] NPEs leverage the costs of defending a suit to obtain licensing agreements on weak infringement claims. Between 1985 and 2004, alleged infringers averaged $2.46 million in defense fees in patent litigation suits that continued through trial, whereas alleged infringers only averaged $57,000 in defense fees in suits resolved before going to trial.[112] Because of the costs associated with defending an infringement suit and unclear patent boundaries, approximately seventy percent of all patent cases settled in the early 2000s.[113] NPEs exploit the fact that companies have higher discovery costs and an incentive to settle in nuisance suits for any amount up to the anticipated defense costs.[114]

Further, while defensive patent aggregation may give companies the ability to neutralize potential suits against other practicing companies, NPEs do not fear countersuit.[115] For aggregation to deter suits, two or more companies must have symmetry of exposure that maintains a "patent stalemate."[116] If two companies each own extensive patent portfolios and produce products, the risk of countersuit deters patent assertion.[117] However, unlike practicing companies, NPEs do not face the same retaliatory risks because they do not make, use, import, or sell any infringing product or technology.[118] An NPE's primary risks in patent litigation are that (1) the court shifts the fees to hold the NPE liable for the defendant's expenses,[119] or (2) the court invalidates the asserted patent,

enough that licensees decide it is not worth going to court." Mark A. Lemley, *Rationale Ignorance at the Patent Office*, 95 NW. U. L. REV. 1495, 1517 (2001).

111. John R. Allison et al., *Patent Quality and Settlement Among Repeat Patent Litigants*, 99 GEO. L.J. 677, 693–94 (2011) (exposing that if default judgments are not taken into account, NPEs win only 8% of their cases).

112. *See* James E. Bessen & Michael J. Meurer, *The Private Costs of Patent Litigation* 16 (B.U. Sch. L., Working Paper Series, Law & Econ. Working Paper No. 07-08, 2008), *available at* http://ssrn.com/abstract_id=983736.

113. *See* Jay P. Kesan & Gwendolyn G. Ball, *How Are Patent Cases Resolved? An Empirical Examination of the Adjudication and Settlement of Patent Disputes*, 84 WASH. U. L. REV. 237, 274 (2006).

114. *See* David Rosenberg & Steven Shavell, *A Model in Which Suits are Brought for Their Nuisance Value*, 5 INT'L REV. L. & ECON. 3, 4–5 (1985).

115. Schultz & Urban, *supra* note 43, at 7–8.

116. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 317.

117. *See id.* at 317–18.

118. *Id.*

119. 35 U.S.C. § 285 (2012) provides that in "exceptional cases" the court may award reasonable attorney fees to the prevailing party. NPEs face more risk from fee-shifting after *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, 134 S. Ct. 1749 (2014). *See infra* Part IV.

foreclosing any future assertion of the invalidated patent by the NPE.[120] Because of these limited risks, NPEs exploit the asymmetrical exposure and cost of litigation to their advantage.[121]

As a result, by the mid-2000s, NPEs brought around twenty percent of total patent infringement suits and became prominent players in the patent field.[122] For example, Acacia Research Corporation ("Acacia"), a publicly traded company, monetizes purchased patents[123] and enforces patents owned by individual inventors or companies.[124] From 1993 to 2008, Acacia generated $410 million in revenues and litigated 308 lawsuits.[125]

Additionally, Intellectual Ventures ("IV") became a feared NPE during this time with an estimated portfolio of over 30,000 patents.[126] IV portrays its primary purpose as a patent intermediary that facilitates patent transactions between individual inventors and manufacturing entities.[127] However, Robin Feldman and Tom Ewing identified 1,276 shell companies that IV operated to hide nearly eight thousand U.S. patents and three thousand pending applications.[128] IV's use of shell companies does not promote its claimed role as a "patent intermediary." Conversely, the use of shell companies enhances IV's leverage in licensing and assertion campaigns by hiding patents until after companies have committed to the underlying technology.[129]

In addition to the threat of NPEs, the continuing influx of patents exacerbated patent thickets. These obstacles prompted further additions to the defensive patent playbook.

120. Allison et al., *supra* note 111, at 678-80.

121. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 317–18.

122. Colleen V. Chien, *Patent Trolls by the Numbers* (Santa Clara Univ., Working Paper Series, Legal Studies Research Paper No. 08-13, 2013), *available at* http://ssrn.com/abstract=2233041.

123. Orr, *supra* note 36, at 525–26.

124. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 328–29.

125. *Id.* at 329.

126. Feldman & Ewing, *supra* note 99, at 4.

127. *Historical Perspective on the Patent Market*, INTELLECTUAL VENTURES INSIGHTS BLOG (July 1, 2013), http://www.intellectualventures.com/insights/archives/historical-perspective-on-the-patent-market.

128. Feldman & Ewing, *supra* note 99, at 4.

129. Orr, *supra* note 36, at 543–44.

B. DEFENSIVE PLAYS IN THE WAKE OF THE DOT-COM BUBBLE

While companies continued to use the plays from Part I,[130] four additional plays entered the defensive patent playbook during this era: lobbying for doctrinal changes, public disclosure, patent pledges, and RPX defensive protection. Public disclosure and patent pledges provide companies with further methods of navigating patent thickets but do not provide additional defense from NPEs. Companies attempted to address the NPE threat that emerged in the wake of the dot-com bubble by seeking substantive changes in the law.

1. Lobbying for Changes in Patent Doctrines

As a general defensive strategy, companies with significant resources may attempt to change the law. These companies can seek doctrinal changes from the legislative branch by funding advocacy groups and from the judicial branch by filing amicus curiae briefs.[131] While this play will not mitigate imminent threats, changes in patent law doctrines may have the greatest effect on the future patent landscape.

Companies may fund lobbying groups that will advocate on behalf of their interests. Lobbying has been a method of change in this country since the founding of the Republic[132] and has become central in patent law reform. For example, when the patent system began to accumulate the obstacles discussed above, Congressman Lamar Smith introduced the Patent Reform Act of 2005, which he called "the most comprehensive change to U.S. patent law since Congress passed the 1952 Act."[133] In response to reform efforts, many large companies allocated substantial money to form and fund lobbying groups, such as the Coalition for Patent Fairness and the Coalition for 21st Century Patent Reform.[134] These

130. *See supra* Part I.

131. "Amicus curiae" refers to "someone who is not a party to a lawsuit but who petitions the court or is requested by the court to file a brief in the action because that person has a strong interest in the subject matter." BLACK'S LAW DICTIONARY 102 (10th ed. 2014)

132. William N. Eskridge, Jr., *Federal Lobbying Regulation: History Through 1954, in* THE LOBBYING MANUAL: A COMPLETE GUIDE TO FEDERAL LOBBYING LAW AND PRACTICE 6 (3d ed. 2005).

133. *See Amendment in the Nature of a Substitute to H.R. 2795, The "Patent Reform Act of 2005"*, *Hearing on H.R. 2795 Before the Subcomm. On Courts, the Internet, and Intell. Prop. Of the H. Comm. On the Judiciary*, 109th Cong. 214 (2005) (statement of the Hon. Lamar Smith, Chairman of the Subcommittee).

134. *See* Candace Lombardi, *Tech Firms to Lobby for Patent Litigation Reform,* ZDNET NEWS (May 11, 2006, 1:22 PM), http://www.zdnet.com/article/tech-firms-to-lobby-for-patent-litigation-reform/; IPFrontline, *New Coalition Seeks to*

lobbying groups represented both the information technology and biomedical industries, which had divergent interests.[135] Eventually, after millions of dollars and significant compromises, the Patent Reform Act of 2005 evolved to become the America Invents Act ("AIA"), which strengthened companies' defensive position.[136] However, the Supreme Court addressed many of the proposed changes before the AIA was signed into law.

In addition to legislative lobbying, companies may seek to influence patent doctrines through amicus curiae briefs. The influence of amicus curiae briefs is debatable,[137] but companies throughout the 2000s filed these briefs in support of their interests. For example, in 2006 and 2007, companies filed extensive amicus curiae briefs in substantive patent law cases before the Supreme Court. In *eBay Inc. v. MercExchange, L.L.C.*, a number of technology companies filed briefs supporting eBay's certiorari petition.[138] Ultimately, the Court's opinion increased the difficulty of obtaining a permanent injunction to prevent further use of infringing technology.[139] The decision essentially eliminated NPEs' ability to

Protect American Innovation, IP FRONTLINE (Mar. 23, 2007), http://www.ipfrontline.com/depts/article.asp?id=14571&deptid=8.

135. *See generally* WENDY H. SCHACHT, CONG. RESEARCH SERV., RL33367, PATENT REFORM: ISSUES IN THE BIOMEDICAL AND SOFTWARE INDUSTRIES (2006).

136. *See* Tracie L. Bryant, Note, *The America Invents Act: Slaying Trolls, Limiting Joinder,* 25 HARV. J.L. & TECH. 687, 688–90 (2012); Wes Klimczak, *IP: How the AIA Has Affected Patent Litigation*, INSIDE COUNSEL MAG. (June 18, 2013), http://www.insidecounsel.com/2013/06/18/ip-how-the-aia-has-affected-patent-litigation; *see also infra* Part III (discussing *inter partes* reviews).

137. *See generally* Joseph D. Kearney & Thomas W. Merrill, *The Influence of Amicus Curiae Briefs on the Supreme Court*, 148 U. PA. L. REV. 743 (2000).

138. The companies presenting the briefs included Yahoo!, Intel, Microsoft, Oracle, Micron, Research-in-Motion, and Nokia. Dennis Crouch, *Review: EBay v. MercExchange Amici Briefs*, PATENTLY-O (Jan. 30, 2006), http://patentlaw.typepad.com/patent/2006/01/ebay_v_mercexch.html; *see, e.g.*, Brief for Yahoo! Inc., as Amicus Curiae in Support of Petitioner, eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388 (2006) (No. 05-130).

139. *eBay*, 547 U.S. 388 (2006):

> According to well-established principles of equity, a plaintiff seeking a permanent injunction must satisfy a four-factor test before a court may grant such relief. A plaintiff must demonstrate: (1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.

Id. at 391.

threaten companies with injunctions, thereby reducing their leverage.[140] Furthermore, in *KSR International Co. v. Teleflex, Inc.*, numerous companies filed amicus curiae briefs.[141] The holding in this case broadened the applicability of the obviousness test, ruling that obviousness is not "confined by a formalistic conception of the words teaching, suggestion, and motivation."[142] The decision made the obviousness claim easier to assert as an invalidity defense and seemingly diminished the presumption of patent validity under 35 U.S.C. § 282. It remains unclear what, if any, effect the amicus curiae briefs had on the Court's holdings, but both decisions increased defendants' leverage in patent litigation.

In conclusion, companies may seek to change patent law doctrines through lobbying and amicus curiae briefs. The results of lobbying develop slowly, and the value gained from amicus curiae briefs is difficult to measure. However, companies that successfully affect substantive patent doctrines shift their exposure in the patent landscape. These efforts will likely be coupled with other defensive plays, such as public disclosure.

2. Public Disclosure

Public disclosure erects a "bulwark against future patent threats" by creating prior art that patent applications must overcome.[143] Patent examiners evaluate patent applications by searching the state of the prior art.[144] When parties disclose information, the disclosure becomes part of the existing prior art.[145] Because no patent may be granted for knowledge within the prior art or any obvious improvement thereupon, public

140. Courts have granted injunctions to NPEs in a handful of cases. *See, e.g.*, Joyal Prods., Inc. v. Johnson Elec. N. Am., Inc., No. 04-5172(JAP), 2009 WL 512156 (D.N.J. Feb. 27, 2009) (granting an injunction in favor of a NPE that had previously practiced the patent); Commonwealth Scientific & Indus. Research Org. v. Buffalo Tech. Inc., 492 F. Supp. 2d 600 (E.D. Tex. 2007) (granting an injunction to a research institution of the Australian government).

141. The companies presenting briefs in support of the petitioner included Intel, Micron, Cisco, GM, Time Warner, and Viacom. Dennis Crouch, *KSR Shifts Obviousness Debate to "Mere Aggregations" and Presumptions of Non-Obviousness*, PATENTLY-O (Nov. 20, 2006), http://patentlyo.com/jobs/2006/11/ksr_shifts_obvi.html. Other companies filed briefs in support of neither party: IBM, Ford Motor Company, and Daimler Chrysler. Predictably, Intellectual Ventures filed a brief in support of respondent. *Id.*

142. KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 419 (2007).

143. Schultz & Urban, *supra* note 43, at 27.

144. Prior art may be defined as references or knowledge available to the public before a specified date. *See generally* Robert P. Merges, *Priority and Novelty Under the AIA*, 27 BERKELEY TECH. L.J. 1023 (2012).

145. The AIA enhances the power of public disclosure because other inventors can no longer swear behind disclosed references. 35 U.S.C. § 102(b) (2012).

disclosure affects the patentability of others' inventions.[146] Companies use public disclosure as a salvage strategy or as a tactic to reduce downstream transaction costs. There are multiple methods of implementing this play, each with their own benefits and limitations.

a) Public Disclosure Benefits

Companies impede competitors from obtaining patents and reduce the patent thicket through the public disclosure play. They implement this strategy in two different scenarios. First, companies may use public disclosure as a salvage strategy when their research leads to an unpatentable invention or a "patentable invention that is of limited commercial value."[147] Even if their research does not yield valuable patent rights, companies affect the patentability of others' inventions by altering the state of the prior art.[148]

In addition, companies may use public disclosure to reduce downstream transaction costs. As the value of patent rights increased in the 1990s, the value of preempting patent rights increased.[149] As a result, entities attempt to obtain preempting patent rights.[150] These entities profit by controlling the building blocks that further cumulative innovation can build upon.[151] Practicing companies may utilize public disclosure to prevent others from obtaining preemptive patent rights and consequently eliminate prohibitive transaction costs. By entering information into the public domain, companies strategically "forgo property rights to reduce downstream transaction costs."[152]

For example, in the late 1990s, scientists used single nucleotide polymorphisms ("SNPs") as diagnostic tools that functioned as "disease markers."[153] SNPs could have created "a potential anticommons" because in theory many SNPs could be present in a gene that causes a disease.[154] Any organization researching a gene in order to create a therapy would

146. *See* Gideon Parchomovsky, *Publish or Perish*, 98 MICH L. REV. 926, 928 (2000).

147. Wendell Ray Guffey, *Statutory Invention Registration: Defensive Patentability*, 16 GOLDEN GATE U. L. REV. 291, 292 (1986).

148. *See* Parchomovsky, *supra* note 146, at 928.

149. *See* Merges, *supra* note 87, at 185–86.

150. *Id.*

151. The *In re Fisher* case now prevents the patenting of research intermediaries that provide no practical benefit to the public by ruling that these intermediaries contain no specific and substantial utility. 421 F.3d 1365, 1367 (Fed. Cir. 2005).

152. Merges, *supra* note 87, at 191.

153. *Id.* at 189.

154. *Id.* at 189–90.

need to license every patented SNP associated with that gene.[155] Ten major pharmaceutical companies responded by creating the SNP Consortium for the purpose of entering SNPs into the public domain.[156] The SNP Consortium set out to disclose 300,000 SNPs in two years, but it surpassed this goal by entering nearly 1.4 million SNPs into the public domain by the end of 2001.[157]

b) Public Disclosure Limitations

The public disclosure play may eliminate companies' ability to obtain patent rights. Under 35 U.S.C. § 102, inventors must file a patent application within one year of public disclosure.[158] Therefore, unless a patent application is filed within one year of disclosure or as the method of disclosure, companies lose their ability to seek patent rights by utilizing a public disclosure strategy.

This bar may become important because the public disclosure play sometimes relies on third parties. If a company wants to use public disclosure to reduce downstream transaction costs, the company must ensure that others in the industry will make similar public disclosures before implementing this tactic because once one party begins preempting, "all will want to obtain blockade positions."[159] However, the risk of losing the ability to obtain patent rights can be mitigated by a strategic disclosure strategy.

If a company decides to use public disclosure, it must determine the most effective method of implementing the strategy. This Note analyzes three methods of entering information into the public domain: (1) creating a printed publication, (2) filing a utility patent application, and (3) prosecuting a patent application and dedicating the patent to the public. Each method contains its own limitations.

Parties may disclose their technology by creating a printed publication. The PTO considers a reference to be a printed publication "upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable

155. *Id.*

156. *Id.* at 190.

157. Gudmundur A. Thorisson & Lincoln D. Stein, *The SNP Consortium Website: Past, Present and Future*, 31 NUCLEIC ACIDS RES. 124 (2003).

158. 35 U.S.C. § 102(a)–(b)(1) (2012).

159. *See* Richard A. Epstein, *Steady the Course: Property Rights in Genetic Material* 48–49 (Univ. of Chi. L. Sch., John M. Olin L. & Econ. Working Paper No. 152, 2003), *available at* http://ssrn.com/abstract_id=317101.

diligence, can locate it."[160] Therefore, a party could create a "printed publication" by publicly posting information on the internet.

Creating a printed publication enables quick and cheap disclosure. However, in order for the disclosure to be considered prior art, the patent examiner must learn about it, and the disclosed information must be described in a comprehensible manner.[161] Patent examiners spend on average only eight to eighteen hours to complete review work for each patent.[162] Therefore, in order for this method of public disclosure to be effective, companies must make the printed publications easily searchable, and the inventors must provide comprehensible disclosures in the publications.

Alternatively, parties may disclose information through the PTO by filing a patent application. Patent applications become prior art as of their filing date[163] and are published eighteen months after the filing date or earlier if requested.[164] Thus, a party may choose to file a patent application to create prior art and then later abandon the application.[165]

Filing a patent application as a method of disclosure enhances the effectiveness of the play and mitigates the risk of losing patent rights. First, it increases the patent examiner's ability to find the disclosure. Also, because it generally takes over one year for a patent application to become abandoned,[166] companies utilizing this method have more time to withdraw from the public disclosure strategy without forfeiting their ability to gain patent protection.

Nevertheless, filing a patent application to disclose has its own drawbacks. First, it may become expensive to file an application for each

160. *In re* Wyer, 655 F.2d 221, 226 (C.C.P.A. 1981) (citing I.C.E. Corp. v. Armco Steel Corp., 250 F. Supp. 738, 742–43 (S.D.N.Y. 1966)).

161. Schultz & Urban, *supra* note 43, at 27–28 (noting that organizations have attempted to build a repository for prior art to help lower the search costs associated with finding the published information for both defense lawyers and the PTO).

162. *Id.* at 29.

163. 35 U.S.C. § 102(a).

164. 35 U.S.C. § 122(b)(1)(A) (2012).

165. Prior to the implementation of the AIA, 35 U.S.C. § 157 (2006) allowed inventors to file a Statutory Invention Registration ("SIR") that prevented others from obtaining a patent but lacked any enforceability right.

166. Companies must fail to reply to an Office Action from the PTO before the application is abandoned. 35 U.S.C. § 133 (2012). The type of technology of the invention dictates the response time for an Office Action. The PTO provides estimates of the time until a first Office Action on its website, at http://www.uspto.gov/cgi-bin/fao_calc/fao_calc.pl?au=&submit=Search+by+
Art+Unit.

disclosure. The PTO currently charges $280, or $140 for a small entity, to file a utility patent application.[167] Furthermore, while a patent application becomes prior art as of its filing date in the United States,[168] the patent application may not serve as prior art internationally until published.[169] Companies seeking to disclose information internationally may choose to simultaneously create a printed publication online, rather than relying on the PTO to publish their application in a timely manner.

Finally, companies may prosecute patents and subsequently dedicate the patent to the public.[170] However, companies likely would choose alternative methods of public disclosure due to the cost associated with prosecuting a patent application.

c) Summary of the Public Disclosure Play

Companies primarily consider implementing a public disclosure play in two scenarios. First, companies may utilize public disclosure to supplement prior art as a salvage strategy when an invention is unpatentable or of limited commercial value.[171] Second, where the value in preventing preemption exceeds the value of patent rights, companies may consider utilizing public disclosure to eliminate downstream transaction costs associated with excessive fragmentation of patent rights.[172] Before using this tactic, however, companies must ensure that others in the industry commit to making similar public disclosures because once one company begins preempting, other companies may abandon the public disclosure strategy.[173] Ideally, in order to protect patent rights, companies implementing public disclosure would simultaneously create a comprehensible "printed publication" and file a patent application that will subsequently be abandoned.

3. Patent Pledges

In addition to public disclosures, companies may use patent pledges as a defensive tactic. Patent pledges are "promises by patent holders not to enforce their patents under certain conditions."[174] These pledges are

167. 37 C.F.R. § 1.16(a) (2013).

168. 35 U.S.C. § 102(a)(2) (2012).

169. *See, e.g.*, Alex Zhang, *Key Considerations for Patent Strategies in China*, IPWATCHDOG (Nov. 6, 2011), http://www.ipwatchdog.com/2011/11/06/key-considerations-for-patent-strategies-in-china/id=20241/.

170. 35 U.S.C. § 253(b) (2012).

171. Guffey, *supra* note 147, at 292.

172. *See* Epstein, *supra* note 159, at 48–49.

173. *See id.*

174. Schultz & Urban, *supra* note 43, at 30.

typically announced publicly and do not require reciprocal agreements by other inventors or companies.[175] Parties who utilize patent pledges do so in reliance on the legal doctrines of contract law, estoppel, or implied license.[176]

Since ownership of the pledged patents remains with the promisor, these patents likely retain their defensive utility against other practicing companies in the future. Further, because NPEs are not exposed to countersuit, a patent pledge does not affect NPE litigation.[177] Thus, patent pledges do not reduce or modify the promisor's exposure to patent litigation, but they do provide practicing companies with alternative benefits.

a) Patent Pledge Benefits

Patent pledges provide consumers assurance of an open network, influence the development of standards, and increase innovation by startup companies. First, patent pledges provide consumers assurance that the pledged patents will not hinder the adoption of market-wide interoperability standards.[178] In markets with network externalities, assurances of interoperability possess significant power. A patent pledge can eliminate the threat of dominance present in a proprietary system and assures users of a commitment to interoperability, which influences consumers' views of the expected network size.[179] In network markets, consumers base purchases of durable products on the expected size of the network.[180] Thus, assurances to consumers may be a powerful tactic

175. *Id.*

176. *Id.* (explaining that an implied license requires the pledgee to show that the pledgor intended to license the patent for a specific use and estoppel only provides a defense to patent infringement when the alleged infringer can show that he knew of the patent pledge and reasonably relied upon it).

177. *Id.* at 7–8.

178. Jorge L. Contreras, *Tesla Motors and the Rise of Non-ICT Patent Pledges*, PATENTLY-O (June 16, 2014), http://patentlyo.com/patent/2014/06/motors-patent-pledges.html.

179. *See* Jorge L. Contreras, *A Market Reliance Theory for FRAND Commitments and Other Patent Pledges*, __ UTAH L. REV. (forthcoming 2015) (manuscript at 4–5), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309023; *see also* Merges, *supra* note 87, at 193 (explaining that a public domain operating system "comes without the threat of leverage and dominance that are always present with a proprietary operating system").

180. Michael L. Katz & Carl Shapiro, *Network Externalities, Competition and Compatibility*, 75 AM. ECON. REV. 424, 426 (1985).

because systems that are expected to be popular will be more popular for that reason.[181]

IBM's support of Linux provides an example. IBM focused its business on the sale of "infrastructure" software, including network management, collaboration tools, and databases.[182] In the late 1990s, IBM recognized that its computer operating system, OS/2, could not compete with Microsoft's Windows operating system.[183] If Microsoft controlled the personal computer operating system, IBM would have suffered financially because the operating system acted as an "input into its main product lines" of infrastructure software.[184] IBM responded by supporting the open source Linux platform and announced it would invest one billion dollars to make Linux suitable for enterprise use.[185] IBM continued its commitment by making a patent pledge of five hundred patents in 2005 that "made the headlines of every major technology-related news publication."[186] The patent pledge assured users that they could commit to Linux without the threat of dominance present in a proprietary operating system such as Microsoft Windows.[187] Ultimately, the assurance provided by IBM's patent pledge likely altered the competitive landscape and improved IBM's position in the market.

Furthermore, companies may use the assurances of patent pledges to influence the competitive environment in which they operate by promoting standards or preventing their adoption. In markets with network externalities, a natural tendency toward standardization exists.[188] Patent pledges commit the network to openness and concede any attempt for proprietary control over the standard.[189] Because the assurance of

181. Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON. PERSP. 93, 94 (1994) [hereinafter Katz & Shapiro, *Systems Competition and Network Effects*].

182. Merges, *supra* note 87, at 192.

183. Dirk Riehle, *The Economic Case for Open Source Foundations*, IEEE COMPUTER, Jan. 2010, at 95.

184. Merges, *supra* note 87, at 192–93.

185. Wen Wen et al., *Patent Commons, Thickets, and the Open Source Software Entry by Start-up Firms*, (Nat'l Bureau of Econ. Research, Working Paper No. 19394, 2013), http://www.nber.org/papers/w19394.pdf.

186. Andrés Guadamuz González, *Open Science: Open Source Licenses in Scientific Research*, 7 N.C. J. L. & TECH. 321, 360–61 (2006).

187. Merges, *supra* note 87, at 186 (stating that IBM's investment in the Linux system "amounts to a credible commitment that no one—including IBM itself—will be able to exercise the sort of hold-up power that comes with exclusive ownership of property rights in a computer operating system").

188. Katz & Shapiro, *Systems Competition and Network Effects*, *supra* note 181, at 105.

189. Merges, *supra* note 87, at 193.

openness alters consumers' expectations as to the size of the network, patent pledges influence the adoption of a standard. For instance, IBM utilized its patent pledge to promote the Linux operating system, which prevented Microsoft's Windows system from becoming the industry standard.[190]

Finally, established companies may utilize a patent pledge to promote increased innovation by startup companies. Patent thickets can increase at least three costs for startups: (1) costs of inventing around others' patent rights, (2) costs of acquiring patents owned by others, and (3) costs of infringement, which includes licensing costs and litigation costs.[191] Patent pledges may reduce these costs for startup companies entering the market by clearing a portion of a patent thicket.[192]

These reduced costs may promote increased funding of startup companies. When applying for venture capitalist funding, a startup typically reports ongoing litigation.[193] A litigation risk or the potential for licensing demands deters some investors who see the exposure as a limit to potential revenue.[194] Economist Catherine Tucker estimates that venture capitalist investments in new innovations and startup companies over the past five years would likely have been $109 million higher if not for the excessive patent litigation by "non-frequent litigators" and $22.772 billion higher if not for litigation brought by "frequent litigators."[195]

Thus, the patent pledgor may "forego [sic] potential opportunities to license their [intellectual property rights] in hopes of increasing innovative activity that will spur demand for complementary products and services from which the contributor can appropriate value."[196] For example, IBM strategically employed a patent pledge to increase innovative activity by programmers within the Linux platform. The patent pledge spurred the development of Linux, resulting in increased demand for IBM's infrastructure software.[197] While patent pledges provide companies with multiple benefits, the play contains some limitations.

---

190. *See id.* at 123.

191. *See* Wen, *supra* note 185, at 5.

192. *Id.* at 2.

193. Catherine Tucker, *The Effect of Patent Litigation and Patent Assertion Entities on Entrepreneurial Activity* 9–10 (2014), *available at* http://ssrn.com/abstract=2457611.

194. *Id.* at 10 (recognizing that "there may be other positive effects of patent litigation on VC investment that should be traded off against the potential for these negative effects").

195. *Id.* at 36.

196. Wen, *supra* note 185, at 29.

197. Merges, *supra* note 87, at 192–93.

b) Patent Pledge Limitations

Companies should be aware of a patent pledge's inability to alleviate concerns regarding the enforceability and revocability of the pledge.[198] In theory, after making a patent pledge, companies cannot assert patent rights against others that meet the conditions of the pledge.[199] Thus, the pledgor has no ability to offensively monetize the pledged patents. However, no caselaw has interpreted the enforceability of patent pledges or their revocability.[200] According to some scholars, patent pledge enforceability remains vulnerable to attack because the pledges rely on the doctrines of estoppel and implied license.[201] Further, the revocability of patent pledges remains a concern.[202] Without a reciprocal agreement to keep the pledged technology open, a pledge could theoretically be withdrawn.[203] The pledgor may change its business strategy, or the pledged patents may be transferred to a successor that chooses not to honor the patent pledge.[204] The determination of the enforceability of a pledge and whether the pledge can be revoked influences both the effectiveness of the patent pledge and the value of the patents.

c) Summary of the Patent Pledge Play

Companies participating in a market with network externalities may consider the patent pledge as a tactic to (1) provide consumers assurance of an open network, (2) influence standardization within the market, and (3) increase innovative activity by startup companies. A company with patents used for primarily defensive purposes must determine if the value derived from the patent pledge exceeds the value of maintaining unencumbered patents for future use. If a company's business model depends on the monetization of patents, the potential value gained through the patent pledge must be weighed against the income derived from patent monetization.

198. *See* Schultz & Urban, *supra* note 43, at 32; *see also* Florian Mueller, *IBM Breaks the Taboo and Betrays its Promise to the FOSS Community*, FOSS PATENTS (Apr. 6, 2010), http://fosspatents.blogspot.com/2010/04/ibm-breaks-taboo-and-betrays-its.html.

199. *See* Schultz & Urban, *supra* note 43, at 31. Searches in Westlaw and Lexis confirmed Jason Schultz and Jennifer Urban's assertion that no court has interpreted a patent pledge, as of January 25, 2015.

200. *Id.*

201. *Id.* at 32.

202. *Id.*

203. *Id.*

204. *Id.*

Because the contours of patent pledge enforceability and revocability have not been clearly defined, companies implementing technology included in patent pledges must consider the risk that a pledged patent will be revoked or transferred to an offensive entity. Companies may consider seeking a license from the pledgor, if feasible, to eliminate this risk. However, if the patent pledge garnered significant publicity, the risk of revocation may be mitigated by the reputational harm that would result.

4. Defensive Protection: RPX

In addition to self-implemented plays, companies may utilize a third party for added protection. In 2008, RPX Corporation ("RPX") began offering a "Defensive Patent Aggregation" service to reduce companies' exposure to patent litigation.[205] RPX monitors patents available for sale and acquires patents that may be asserted against members or potential members.[206] RPX licenses these patents to companies that pay the annual subscription fee to become a member.[207] Thus, RPX protects members from immediate threats of patent litigation from other practicing companies and NPEs.

However, once a license has been provided, RPX may sell the acquired patents to practicing companies or NPEs, which has been called a "catch and release method."[208] Releasing patents seems to fuel, rather than deter, the threat of patent litigation. RPX does not assert patents[209] but indirectly poses a significant threat to practicing companies. Suppose RPX approaches Company *Z* and asks them to become a member. Company *Z* rejects the offer. RPX can sell a patent to an aggressive third party that will bring suit against Company *Z* so that the next time Company *Z* will be more compliant with RPX's request. One company has already claimed that RPX is guilty of extortion, racketeering, and wire fraud.[210]

RPX has recently started to offer patent litigation insurance products.[211] These insurance products attempt to transform "the expensive

205. RPX Corporation, Registration Statement (S-1) (Sept. 2, 2011).
206. *Id.*
207. *Id.*
208. David Hetzel, *Embracing the New IP Reality*, INTELL. ASSET MGMT. MAG. May/June 2010, at 32.
209. Registration Statement (S-1), *supra* note 205.
210. Patrick Anderson, *Patent Aggregator RPX Accused of Extortion, Racketeering & Wire Fraud*, GAMETIME IP (May 31, 2011), http://gametimeip.com/2011/05/31/patent-aggregator-rpx-accused-of-extortion-racketeering-wire-fraud/.
211. *Welcome to RPX Insurance Services*, RPX INS. SERVS., http://www.rpxcorp.com/insurance/ (last visited Nov. 8, 2014).

uncertainty of NPE litigation into a manageable and predictable cost of business."[212] However, it appears only a handful of companies have chosen to utilize the insurance products.[213]

In conclusion, companies may utilize the RPX defensive protection play to supplement other patent strategies. However, RPX's "defensive patent aggregation" service provides limited protection from litigation exposure and creates additional threats in the patent system. These services provide companies with various tools, but the trend of increased patent litigation has not subsided.

III. CURRENT LANDSCAPE

Excessive litigation of patent rights has caused the media,[214] legal scholars,[215] and President Obama[216] to question the validity of the current patent system. The obstacles of prior eras have accumulated in the current patent landscape. Practicing companies fight "patent wars" in areas of dense patent thickets,[217] and the number of NPE suits continues to grow.[218] Data provided by RPX indicates that in 2012, NPEs brought sixty-two percent of patent infringement suits.[219] In addition to the lingering threats, some practicing entities in the current landscape shifted from patent aggregation to patent monetization. As a result, companies

212. *Id.*

213. Boris Marjanovic, *RPX Corporation: A Cheap and Misunderstood Patent Company With a Moat*, SEEKING ALPHA (Aug. 30, 2013), http://anorthinvestments.com/2014/09/23/rpx-corporation-a-cheap-and-misunderstood-patent-company-with-a-moat/.

214. *See 441: When Patents Attack!*, THIS AMERICAN LIFE (July 22, 2011), http://www.thisamericanlife.org/radio-archives/episode/441/when-patents-attack; *Patent Trolls: How Some Say They're Hurting U.S. Economy* (CBS News television broadcast Dec. 21, 2012).

215. *See generally* DAN L. BURK & MARK A. LEMLEY, THE PATENT CRISIS AND HOW THE COURTS CAN SOLVE IT (2009); Peter S. Menell, *A Method for Reforming the Patent System*, 13 MICH. TELECOMM. & TECH. L. REV. 487 (2007).

216. *See* Barack Obama, President of the United States, State of the Union Address (Jan. 28, 2014), 2014 DAILY COMP. PRES. DOC. NO. 00050 (urging Congress to pass a patent reform bill); David Kravets, *History Will Remember Obama as the Great Slayer of Patent Trolls*, WIRED (Mar. 20, 2014, 6:30 AM), http://www.wired.com/2014/03/obama-legacy-patent-trolls/.

217. *See* Terry Ludlow, *Trends in US Patent Litigation*, INTELL. ASSET MGMT. MAG., Sept.–Oct. 2011, at 15; Jacob Goldstein, *The Smartphone Patent War, In 1 Graphic*, NPR: PLANET MONEY (Aug. 17, 2011), http://www.npr.org/blogs/money/2011/08/17/139723088/the-smartphone-patent-war-in-1-graph (showing an illustration of smartphone patent cases).

218. Chien, *Patent Trolls by the Numbers*, *supra* note 122.

219. *Id.*

have resorted to (1) old plays in the current landscape, (2) modified plays, and (3) new entries to the defensive patent playbook. However, in order to understand these plays, the progression of the current patent landscape must be evaluated.

A. BACKGROUND: A TRANSITION IN THE USE OF AGGREGATED PATENTS

In light of the high costs associated with acquiring and maintaining patent portfolios, company executives eventually questioned whether their intellectual property assets had the potential to earn income.[220] Many companies had diverted substantial money from their research and development funds to acquire patents,[221] and paid thousands of dollars in maintenance fees for each individual patent.[222] As a result, some companies progressed from defensive patent aggregation to offensive patent monetization.[223]

Monetization of a patent portfolio generates revenue to recoup purchase costs, offset maintenance fees, fund research and development, or enable a change in direction for the company.[224] Monetization by companies occurs in three forms: (1) direct licensing and assertion campaigns against other practicing companies, (2) selling patent assets, and (3) patent privateering.[225]

As previously discussed, IBM and TI pioneered the monetization of patents through licensing and assertion campaigns.[226] With this model in place, other companies that originally built patent portfolios for defensive purposes developed separate licensing and assertion divisions to generate royalties from their portfolios.[227] For example, General Electric, which historically has rarely engaged in licensing, began enforcing patents

220. Lerer, *supra* note 102, at 12.

221. Tom Ewing, *Indirect Exploitation of Intellectual Property Rights by Corporations and Investors: IP Privateering and Modern Letters of Marque and Reprisal*, 4 HASTINGS SCI. & TECH. L.J. 1, 16 (2012).

222. After the PTO grants a patent, patent holders must pay maintenance fees after three and a half years ($1600), seven and a half years ($3600) and eleven and a half years ($7400). 37 C.F.R. § 1.20(e)–(g) (2013).

223. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 325.

224. Orr, *supra* note 36, at 540.

225. *Id.* at 539.

226. *See supra* Part I.

227. Orr, *supra* note 36, at 540.

through its "Trading and Licensing" division.[228] In 2008, General Electric's licensing and assertion campaign brought in $291 million.[229]

In contrast, other companies monetize by selling their patents if offensive assertion is not feasible given the companies' resources and culture.[230] Companies sell ancillary patents to both practicing companies and NPEs with grant-back licenses to eliminate the risk of the patents being used against them.[231] For instance, Acacia claimed that it was approached by "large companies looking to turn their patents into revenue."[232] Similarly, IV contends that practicing companies sell their patents to NPEs.[233] In fact, some companies that previously spoke out about the negative effects of NPEs later sold their patents to those same entities.[234] But most companies remain hesitant, at least publicly, to sell their patents to NPEs because many in the patent field consider this action an "unforgivable sin."[235]

Finally, companies monetize their patent portfolios through patent privateering.[236] Patent privateering occurs when practicing companies sponsor NPEs by transferring full or partial interest in patents to NPEs under revenue sharing arrangements.[237] The privateer, a specialized form of NPE, acts as an agent for these sponsors who are working to achieve corporate goals.[238] The sponsor may attempt to camouflage its involvement.[239] This practice allows companies to indirectly monetize their patent portfolios and alter the competitive landscape, while maintaining

228. Chien, *From Arms Race to Marketplace, supra* note 5, at 322–23.

229. *Id.* at 323.

230. *Id.* at 325.

231. Matthew Fawcett & Jeremiah Chan, *March of the Trolls: Footsteps Getting Louder*, 13 INTELL. PROP. L. BULL. 1, 20 (2008).

232. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 314 (citing ACACIA TECHS., LLC, ACACIA TECHNOLOGIES: LEADER IN PATENT LICENSING AND ENFORCEMENT 3, http://acaciatechnologies.com/docs/CorporateBrochure.pdf (last visited Dec. 17, 2010)).

233. Nathan Myhrvold, *The Big Idea: Funding Eureka!*, HARV. BUS. REV., Mar. 2010, at 41.

234. Chien, *From Arms Race to Marketplace, supra* note 5, at 344 (noting that Micron's counsel spoke publicly about the negative effects of NPEs and later transferred 4,500 patents to an NPE, Round Rock Research LLC).

235. Ewing, *supra* note 221, at 22.

236. *See id.* at 8–9 (explaining that privateering was an effective and cheap method of waging war by enlisting private parties to attack enemy ships and allowing the privateers to keep the proceeds).

237. Orr, *supra* note 36, at 541.

238. Ewing, *supra* note 221, at 24.

239. *Id.* at 5.

focus on their core business and avoiding the risk of retaliation or reputational damage.[240]

While the secretive nature of some patent privateering makes it difficult to trace, it appears that companies provide patent arms to some NPEs.[241] For example, Nokia and Sony each transferred patents to an NPE, Mobile Media LLC, that later asserted those patents against Apple.[242] Similarly, Microsoft transferred patents to a Canadian NPE, Mosaid Technologies, that later brought suit against Google.[243]

In addition to arming NPEs, companies also create NPEs for the purpose of patent privateering. In July 2011, Apple, Microsoft, Research in Motion, Sony, Ericsson, and EMC formed a company, called the Rockstar Consortium, to outbid Google and Intel for Nortel Networks' patent assets.[244] After the purchase, Rockstar Consortium maintained control of the patents and acted as a privateer for its founding companies. Rockstar used Nortel's patents to initiate suits against Google and Samsung. [245]

As these challenges in the patent landscape have accumulated, companies have resorted to old plays, modified tactics, and new strategies.

B. OLD PLAYS IN THE CURRENT LANDSCAPE

Although developed in the mid-1990s, companies continue to use defensive aggregation and patent pledges to enact defensive patent strategies. Companies in today's landscape implement these plays in their original form. The following analysis provides examples of the modern use of this "old play."

1. Defensive Aggregation

Defensive aggregation may be considered an "old play," but companies still utilize the threat of mutual destruction as a defensive tactic in modern practice. For example, Facebook utilized defensive aggregation in litigation against Yahoo!. Just before Facebook's initial public offering,

240. *Id.* at 13–14.
241. Ewing, *supra* note 221 at 38–39.
242. Orr, *supra* note 36, at 541.
243. *Id.* at 541–42.
244. Chia, *supra* note 69, at 213.
245. *See* Kurt Orzeck, *Google, Samsung Sued Over Nortel Search-Engine Patents*, LAW360 (Oct. 31, 2013, 8:59 PM), http://www.law360.com/articles/485409/google-samsung-sued-over-nortel-search-engine-patents?article_related_content=1.

Yahoo! asserted ten patents against Facebook.[246] Facebook counterclaimed using ten of its own patents, four of which it acquired after Yahoo!'s initial assertion.[247] Three months after the initial complaint, Yahoo! and Facebook ended the infringement suit and formed a "strategic alliance."[248]

Similarly, defensive aggregation of patents has been rampant in the ongoing smartphone patent litigation. In October 2009, Nokia sparked a series of suits by asserting that Apple's iPhone infringed their patent rights.[249] The companies settled twenty months later,[250] but the "smartphone war" had begun. Technology giants—such as Microsoft, Google, Apple, Samsung, Research in Motion, and HTC—became participants in a series of patent litigation actions that instigated vast expenditures in patent aggregation.[251] In July 2011, the Rockstar Consortium paid $4.5 billion to outbid Google and Intel for Nortel Networks' six thousand patent assets.[252] Google responded by acquiring 17,000 patents in its purchase of Motorola Mobility for $12.5 billion.[253] Google announced that its primary objective was to protect itself and other business partners from future patent litigation.[254]

246. Complaint for Patent Infringement, Yahoo! Inc. v. Facebook, Inc., No. CV-12-01212, 2012 WL 764479 (N.D. Cal. Mar. 12, 2012).

247. Defendant Facebook, Inc.'s Answer; Counterclaim Against Yahoo! Inc. for Patent Infringement, Yahoo! Inc. v. Facebook, Inc., No. CV-12-01212-JSW, 2012 WL 1094169 (N.D. Cal. Apr. 3, 2012).

248. John Letzing, *Facebook, Yahoo Kiss and Make Up*, WALL ST. J. (July 6, 2012, 6:54 PM), http://online.wsj.com/news/articles/SB10001424052702303684004577511132642631606.

249. *See* Judith Aparri, *Reckoning Smartphone Patent Wars with Nokia, Apple, HTC, Motorola, and Samsung*, INT'L BUS. TIMES (Apr. 7, 2014, 2:12 PM), http://au.ibtimes.com/articles/546903/20140407/apple-vs-samsung-cases-ip-wars-patent.htm#.VEFX5Va0b1o.

250. *See* Ryan Davis, *Apple Pays Up To Settle Nokia Patent Suits*, LAW360 (June 14, 2011, 1:16 PM), http://www.law360.com/articles/251166/apple-pays-up-to-settle-nokia-patent-suits.

251. *See* Aparri, *supra* note 249; *see also* Ludlow, *supra* note 217, at 15.

252. *See* Liam Tung, *Google Settles with Rockstar Consortium Over Nortel Patents*, ZDNET NEWS (Nov. 21, 2014, 1:57 PM), http://www.zdnet.com/article/google-settles-with-rockstar-consortium-over-nortel-patents/.

253. *See* Aaron Pressman, *Now that Google's Selling Motorola, How Much Did it Overpay in 2011?*, THE EXCHANGE – YAHOO! FINANCE (Jan. 29, 2014, 4:42 PM), http://finance.yahoo.com/blogs/the-exchange/google-selling-motorola-phone-business-but-keeping-some-patents-214150173.html (indicating that Google ultimately paid around $4 billion for the 17,000 patent assets after Motorola's assets were sold).

254. Larry Page, *Supercharging Android: Google to Acquire Motorola Mobility*, OFFICIAL GOOGLE BLOG (Aug. 15, 2011), http://googleblog.blogspot.com/2011/08/supercharging-android-google-to-acquire.html.

As illustrated, companies implement defensive aggregation effectively in the modern landscape. However, defensive aggregation is not the only old play that remains in the modern playbook.

2. Patent Pledges

Although developed in the mid-2000s, companies have recently implemented the patent pledge. For instance, Google and Tesla Motors recently used the patent pledge tactic. Google controls the Android operating system used on hundreds of millions of mobile devices worldwide.[255] Android allows users to develop applications, commonly referred to as "apps," and distribute these applications on the Google Play marketplace.[256] In March 2013, Google announced an Open Patent Non-Assert ("OPN") Pledge.[257] The OPN Pledge states that Google will not "sue any user, distributor or developer of open-source software on specified patents, unless first attacked."[258] By October 2014, Google had included 114 U.S. patents and 131 international patents in the OPN Pledge.[259] Just as IBM assured consumers that they could commit to Linux's open source operating system with their patent pledge,[260] Google's OPN Pledge assures users freedom to develop open source software within the Android platform. Additionally, like IBM's pledge increased software for the Linux system,[261] Google's pledge will probably enhance the amount of apps produced for the Android platform.

Similarly, Tesla Motors Inc. ("Tesla") recently implemented a patent pledge. Tesla's chief executive officer, Elon Musk,[262] announced that "Tesla will not initiate patent lawsuits against anyone who, in good faith,

255. Android Developers, *Android, the World's Most Popular Mobile Platform*, http://developer.android.com/about/index.html (last visited Jan. 25, 2015).

256. *Id.*

257. Duane Valz, *Taking a Stand on Open Source and Patents*, GOOGLE OPEN SOURCE BLOG (Mar. 28, 2013), http://google-opensource.blogspot.com/2013/03/taking-stand-on-open-source-and-patents.html.

258. *Id.*

259. *Open Patent Non-Assertion Pledge: Pledged Patents*, GOOGLE OPEN PATENT NON-ASSERTION PLEDGE, http://www.google.com/patents/opnpledge/patents/ (last visited Oct. 4, 2014).

260. Merges, *supra* note 87, at 193.

261. *Id.* at 192–93.

262. Elon Musk co-founded Zip2 and PayPal before his role as CEO of Tesla Motors. *Executive Bios*, TESLA MOTORS INC., http://www.teslamotors.com/executives (last visited Sept. 10, 2014). Musk currently oversees the development of rockets and spacecraft in his position as chief designer at SpaceX. *Id.* In addition, Musk is the non-executive Chairman and principal shareholder of SolarCity. *Id.*

wants to use our technology."[263] At the time of the announcement, Tesla had 172 issued U.S. patents and 123 published pending applications comprised primarily of battery and charging technologies.[264] While Tesla's exact motivations remain unclear, Musk may have sought to assure customers that Tesla would operate on an open network that would not confine consumers to Tesla's charging technology and stations.

Three days after issuing its patent pledge, Tesla met with Nissan and BMW to discuss methods of collaboration and a supercharging network.[265] This meeting led some to speculate that Tesla seeks to make its roadside charging stations or battery packs the industry standard.[266] Yet, it is equally plausible that Tesla's patent pledge intended to ensure that other companies do not exclude Tesla from an interoperable network. Others argue that Tesla seeks to coordinate electric vehicle makers around open standards and allow more companies to enter the industry in order to overcome the gasoline-vehicle standard.[267] Ultimately, while patent pledges can promote or deter the adoption of standards, it is unclear which interoperable component Tesla allegedly seeks to promote as a standard.

Finally, Tesla may be foregoing opportunities to license their charging and battery technology in an effort to spur innovation within the electric vehicle industry. Just as increased innovation within the Linux platform ultimately stimulated demand for IBM's infrastructure software,[268] spurred innovation in battery technology could propel the electric vehicle industry and thereby increase demand for Tesla's cars and batteries.

While the effectiveness of these pledges remains uncertain, companies implement patent pledges in the modern landscape. In addition to these old plays, the modern defensive playbook contains a couple of plays that have been adapted for the current landscape.

---

263. Elon Musk, *All Our Patent Are Belong to You*, TESLA MOTORS INC. (June 12, 2014), http://www.teslamotors.com/blog/all-our-patent-are-belong-you.

264. *Envision IP: Auto Industry May Ignore Tesla Patents*, DELTASIGHT (June 26, 2014), https://www.deltasight.com/tesla-auto-industry-may-ignore-tesla-patents/.

265. Nikki Gordon-Bloomfield, *Nissan, BMW, Look to Adopt Tesla's Charging Standard*, TRANSPORT EVOLVED (June 16, 2014), https://transportevolved.com/2014/06/16/nissan-bmw-look-adopt-teslas-charging-standard/.

266. William J. Watkins, Jr., *Rethinking Patent Enforcement: Tesla Did What?*, FORBES OPINION (July 17, 2014, 1:16 PM), http://www.forbes.com/sites/realspin/2014/07/17/rethinking-patent-enforcement-tesla-did-what/.

267. James Bessen, *History Backs up Tesla's Patent-Sharing*, HARV. BUS. REV. BLOG (June 13, 2014), http://blogs.hbr.org/2014/06/history-backs-up-teslas-patent-sharing/.

268. Merges, *supra* note 87, at 192–93.

C. MODIFIED PLAYS IN THE CURRENT LANDSCAPE

Part I evaluated the open source and RAND strategies implemented in the 1990s. However, these plays have evolved over time. The following analysis traces the development of the open source and RAND plays and provides the current strategies for their utilization. Some of the plays discussed in this Section provide litigation tactics available in very specific situations rather than general defensive strategies.

1. Open Source Licenses II: Patent Provisions and Infection

Open source licenses evolved over time. Because both copyrights and patents can protect software, open source licenses—like the GPL—faced a unique challenge. As software patents became more prevalent in the 2000s, open source licenses began to include reciprocal patent agreements, in addition to copyright provisions, to ensure that software patents could not prevent the use or modification of open source software.[269]

Open source patent provisions prohibit patent assertion by any licensee against the licensor and other downstream licensees of the technology.[270] These provisions are usually structured as either a license to a specified technology or a general covenant not to sue.[271] The Open Source Initiative lists nearly seventy different variations of open source licenses.[272] The majority of the analysis in this Section discusses the GPLv3 and Apache licenses, but the provisions of open source licenses vary.[273]

The GPLv3 prevents the enforcement of patent rights through Section 11 of the GPLv3, which states that "[e]ach contributor grants [any licensee] a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version."[274] However, the provision has caused confusion because it appears directed towards "contributor[s]," which Section 11

269. Phipps, *supra* note 96.

270. Schultz & Urban, *supra* note 43, at 33.

271. *Id.*

272. *Open Source Licenses: Licenses by Name*, OPEN SOURCE INITIATIVE, http://opensource.org/licenses/alphabetical (last visited Jan. 18, 2015).

273. Of the nearly 100,000 projects hosted on Google Code in 2008, 42.6% of these projects utilized the GPLv2/GPLv3 licenses and 25.8% used the Apache license, including the Android operating system. Greg Stein, *Standing Against License Proliferation*, GOOGLE OPEN SOURCE BLOG (May 28, 2008), http://google-opensource.blogspot.com/2008/05/standing-against-license-proliferation.html.

274. GNU General Public License Version 3, GNU OPERATING SYSTEM (June 29, 2007), http://www.gnu.org/licenses/gpl.html.

defines as "copyright holder[s]."[275] If a "contributor" must modify the GPLv3 software to be a "copyright holder," the mere distribution of GPLv3 software without modifications appears not to trigger the license in Section 11.[276] In an attempt to clear confusion regarding the interpretation of Section 11, GPLv3's drafters stated that "non-contributor redistributors remain subject to applicable implied patent license doctrine."[277]

In addition to the patent license, the GPLv3 contains a termination clause that terminates copyright and patent licenses in the event that a user initiates a patent lawsuit against any GPLv3 contributor.[278] These provisions appear to further constrain the enforcement of proprietary technology that includes open source software.

a) Limitations on Effectiveness of Open Source Patent Provisions

The open source patent provisions have some limitations to their effectiveness. Open source licenses lack clarity as to the scope of the patent rights licensed.[279] The drafters of GPLv3 recognized the lack of clarity and subsequently attempted to produce information to assist interpretation.[280] However, because no caselaw has interpreted a patent-related open source provision,[281] uncertainty surrounds the scope and enforceability of the patent licensing provisions.[282] This uncertainty increases the business risk

275. *Id.*

276. Hendrik Schöttle, *Open Source Software and Patents: How the GPLv3 Affects Patent Portfolios*, INT'L LAW OFFICE (Feb. 5, 2013), http://www.internationallawoffice.com/newsletters/Detail.aspx?g=64b59c8c-9677-46eb-97fe-3d22f9fc011e.

277. *What Does "the Program" Mean in GPLv3?*, FREE SOFTWARE FOUNDATION, https://www.gnu.org/licenses/gplv3-the-program.html (last visited Feb. 19, 2015).

278. GNU General Public License Version 3, *supra* note 274.

279. *See* Schultz & Urban, *supra* note 43, at 34; *see also* Andrew Strickland & Amy Chun, *Leveraging Open-Source Software in Patent Litigation*, AM. BAR ASS'N – SEC. OF LITIG. (Sept. 20, 2011), http://apps.americanbar.org/litigation/committees/intellectual/articles/fall2011-leveraging-open-source-software-patent-litigation.html.

280. *See What Does "the Program" Mean in GPLv3?*, *supra* note 277.

281. In 2008, the Federal Circuit held that an open source agreement was enforceable as an express contractual license under *copyright law*; the Federal Circuit found that even without monetary exchange, open source licenses contain consideration because these licenses may generate market share and improve the licensee's reputation. Jacobsen v. Katzer, 535 F.3d 1373, 1379–83 (Fed. Cir. 2008).

282. Schultz & Urban, *supra* note 43, at 33 (recognizing that the validity of open source licensing agreements may be challenged when patents have been transferred to third parties who claim a lack of privity with the original licensee).

in both releasing software and using software licensed by others under the GPLv3.[283]

b) Infection of Open Source Software as a Defensive Tactic

Most technology companies today use software protected under an open source license.[284] These companies face an internal struggle to coordinate their use of open source software with their patent portfolio management.[285] Under a broad interpretation, the GPLv3 grants licenses not only to modified open source software but also to any software that "links" to the open source software.[286] The uncertain scope of open source provisions may drive companies to prohibit use of open source software in proprietary commercial products.[287] Thus, coordination within a company becomes vital to ensure that a proprietary project does not become "infected" with open source software.

If a portion of the plaintiff's software has been infected by open source software, a defendant can use the infection as a defensive tactic in patent litigation. First, the plaintiff may have unknowingly granted the defendant a patent license under the provisions of the open source license, which can be used as a defense to an infringement claim.[288]

Furthermore, the plaintiff's exposure to countersuit increases if the asserted patent includes (1) the defendant's open source software or (2) third-party open source software. If the defendant's open source software infected the plaintiff's software, the plaintiff likely violates the licensing requirements of the open source license.[289] In *Twin Peaks Software Inc. v. Red Hat, Inc.*, Twin Peaks Software ("TPS") asserted patented software against Red Hat.[290] Red Hat initially denied the validity of the patents and claimed they did not infringe—a typical patent defense.[291] However, Red Hat discovered that TPS's proprietary software

283. *See* Majerus, *supra* note 92, at 3.

284. Heather Meeker, *Open Source – The Last Patent Defense?*, OUTER CURVE FOUND. (Feb. 11, 2014), http://www.outercurve.org/blog/2014/02/11/Open-Source--The-Last-Patent-Defense/.

285. *Id.*

286. Majerus, *supra* note 92, at 1–2.

287. *Id.*

288. *See* Meeker, *supra* note 284.

289. *Id.*

290. Defendants Red Hat, Inc.'s and Gluster, Inc.'s Answer and Counterclaims to Plaintiff Twin Peaks Software Inc.'s First Amended Complaint for Patent Infringement at 1, Twin Peaks Software Inc. v. Red Hat, Inc., No. 5:12-CV-00911 RMW; 2012 WL 5403091 (N.D. Cal. Aug. 2, 2012).

291. *Id.* at 4-5.

actually included some of Red Hat's open source software, which triggered the defensive termination clause and created a counterclaim.[292] Red Hat amended its counterclaim to include a violation of the open source license and sought an injunction.[293] Soon thereafter, the case settled.[294]

Further, if a third party has infected a portion of the plaintiff's software, the defendant can use the plaintiff's increased exposure to suits from third parties as a defensive tactic.[295] For example, the defensive termination provision of the Apache 2.0 states that any patent licenses granted to the licensee on open source software shall be revoked if a licensee asserts patent infringement.[296] Therefore, by bringing suit, the plaintiff forfeits any patent licenses it has received from other contributors to the software. Even if the defendant has no direct counterclaim, the plaintiff exposes itself to potential liability from other third parties by filing for patent infringement.[297] This exposure may be utilized as a defensive tactic.

Finally, if the defendant discovers that the plaintiff's software has been infected, the defendant may be able to challenge the inventorship of the patent. Even though the AIA eliminated the inventorship requirement of 35 U.S.C. § 102(f), the PTO has argued that "section 101 continues to restrict the grant of patents to inventors."[298] While the specific use of open source software will dictate the validity of the inventorship argument, defendants have yet another defensive tool that poses additional risk to the patent holder.

---

292. *See* Defendants/Counterclaim-Plaintiffs Red Hat, Inc.'s and Gluster, Inc.'s First Amended Answer and Counterclaims to Plaintiff Twin Peaks Software Inc.'s First Amended Complaint for Patent Infringement at 6, Twin Peaks Software Inc. v. Red Hat, Inc., No. 5:12-CV- 00911 RMW, 2012 WL 5403098 (N.D. Cal. Sept. 13, 2012).

293. *Id.*

294. *See* Meeker, *supra* note 284.

295. *See id.*

296. *Apache License, Version 2.0*, THE APACHE SOFTWARE FOUND. (Jan. 2004), http://www.apache.org/licenses/LICENSE-2.0.html.

297. *See* Meeker, *supra* note 284.

298. Defendant U.S. Patent and Trademark Office's Dispositive Motion at 9, Madstad Eng'g, Inc. v. USPTO, No. 8:12-CV-01589-SDM-MAP, 2012 WL 4936440 (M.D. Fla. Sept. 18, 2012); *but see* Dennis Crouch, *With 102(f) Eliminated, Is Inventorship Now Codified in 35 U.S.C. 101? Maybe, but not Restrictions on Patenting Obvious Variants of Derived Information*, PATENTLY-O (Oct. 4, 2012), http://patentlyo.com/patent/2012/10/with-102f-eliminated-is-inventorship-now-codified-in-35-usc-101.html (discussing the unresolved issues that originate from the elimination of 35 U.S.C. § 102(f)).

c) Summary of the Modified Open Source License Play

Before utilizing open source licenses, companies must evaluate the value of the patent rights against the value gained through implementation and distribution of open source software. Companies must coordinate the use of open source software with their patent portfolio management if they plan to assert their patents. If proprietary projects include open source software, patent rights could be severely limited. However, the effectiveness of patents used *defensively* will be unimpeded due to the termination clauses included in open source licenses. Finally, companies in patent litigation should always determine whether their opponent has been infected with open source software. Infection may provide significant defenses and alter the dynamics of patent litigation.

2. RAND II: Limitations and Breach of Contract Claims

As discussed in Part I, SSOs require RAND commitments to encourage the widespread adoption of standards and prevent SEP holders from utilizing their leverage to demand inflated licensing rates.[299] However, smartphone companies used RAND-encumbered patents in the same manner as other patents were utilized.[300] These companies aggregated SEPs as offensive and defensive weapons.[301] This use of RAND-encumbered patents raised concerns, especially in the smartphone industry where the implementation of a standard in a single smartphone requires hundreds or thousands of SEPs owned by different parties.[302] However, recent court decisions seem to have curbed the abuse of RAND-encumbered patents by limiting the availability of injunctions.

a) Injunction Availability

In *Apple Inc. v. Motorola, Inc.*, the Federal Circuit recognized the difficulty of obtaining an injunction on a RAND-encumbered patent but stated that no "per se rule" against injunctions existed.[303] Judge Reyna declared that the *eBay* framework for analyzing injunctive relief should be

299. *See* U.S. DEP'T OF JUSTICE & USPTO, POLICY STATEMENT ON REMEDIES FOR STANDARDS-ESSENTIAL PATENTS SUBJECT TO VOLUNTARY F/RAND COMMITMENTS 1 n.2 (2013) *available at* http://www.uspto.gov/about/offices/ogc/Final_DOJ-PTO_Policy_Statement_on_FRAND_SEPs_1-8-13.pdf.

300. *See* O'Connor, *supra* note 70.

301. *See id.*

302. James Ratliff & Daniel L. Rubinfeld, *The Use and Threat of Injunctions in the RAND Context*, 9 J. OF COMPETITION L. & ECON. 1, 2 (2013).

303. 757 F.3d 1286, 1331–32 (Fed. Cir. 2014).

utilized to evaluate RAND committed patents.[304] Nevertheless, Judge Reyna recognized that within the *eBay* framework "a patentee subject to FRAND commitments may have difficulty establishing irreparable harm."[305] Thus, the ability to obtain an injunction on a RAND committed patent appears considerably weaker than it would be without the RAND commitment.[306] This decision reduces the threat of SEPs as weapons of mutually assured destruction and reduces patent holders' leverage when licensing SEPs.

But companies may attempt to revoke their RAND commitment. SSOs members generally declare the essentiality of their patents to the standard in their letter of assurance, but the SSOs do not examine whether the patents are actually essential.[307] Thus, companies may argue that their patents are not "essential" to implement the standard under the definition provided in the SSOs' bylaws, which would allow an ordinary infringement suit.[308] But if the patent is essential to the standard, implementers may have a breach of contract defense.

b) Breach of Contract Claim as a Defensive Tactic

The abuse of RAND commitments may lead to a breach of contract claim against a patent holder asserting infringement of a SEP. Because RAND commitments do not arise through statute or regulation, some courts have analyzed RAND commitments as contracts between SEP holders and SSOs, with implementers acting as third-party beneficiaries.[309]

For example, suppose an SEP holder offers an implementer a license for a RAND-encumbered patent essential to the standard. Due to

304. *Id.*

305. *Id.* Some SSOs require members to license under fair, reasonable, and nondiscriminatory terms ("FRAND"). FRAND and RAND are used interchangeably in this Note.

306. Contreras & Gilbert, *supra* note 63, at 31.

307. *See* Thomas F. Cotter, *The Comparative Law and Economics of Standard-Essential Patents and FRAND Royalties*, 22 TEX. INTELL. PROP. L.J. 311, 312 (2014).

308. *See* D. Brian Kacedon et al., *Court Finds Patent Claims Essential to Wi-Fi Standard Because They Cover Technology Required by the Standard and There Are No Commercially or Technically Feasible Noninfringing Alternatives,* FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP LES INSIGHTS (Sept. 17, 2013), http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=d1f3763e-703e-4506-af9f-868bf89bb5d8.

309. *See* Microsoft Corp. v. Motorola, Inc., 864 F. Supp. 2d 1023, 1030 (W.D. Wash. 2012); *see also* Mark A. Lemley & Carl Shapiro, *A Simple Approach to Setting Reasonable Royalties for Standard-Essential Patents*, 28 BERKELEY TECH. L.J. 1135, 1160 (2013).

differing opinions of "reasonable" terms,[310] the implementer rejects the license offer as inconsistent with the RAND commitment. If the SEP holder files suit for patent infringement, the implementer may attempt to enforce the RAND commitment by bringing a breach of contract action.[311] Alternatively, if the SEP holder seeks injunctive relief prior to RAND negotiations, some courts have found that the SEP holder has breached their duty of good faith owed to the contract between the SEP holder and the SSO.[312]

These contractual claims provide multiple defenses. First, the breach of contract claim may be used to limit damages by pleading for relief in the form of a judicially determined RAND rate.[313] Alternatively, or in addition, the alleged infringer may point to the RAND commitment to reduce the likelihood that the court grants injunctive relief.[314] Finally, if the SEP holder sought injunctive relief in foreign courts or the U.S. International Trade Commission, the implementer can file a breach of contract suit to enjoin the SEP holder from enforcing an injunction or exclusion order because the SEP holder breached the duty of good faith and fair dealing.[315] However, these defenses are only available when the plaintiff asserts a RAND-encumbered patent.

c) Summary of the Modified RAND Play

Recent decisions have decreased the threat of SEPs as weapons of mutually assured destruction and reduced patent holders' leverage when licensing SEPs. Therefore, before making a RAND commitment, a company must determine if "reasonable" royalties at higher volumes that result from standardization outweigh the patents' offensive and defensive value and higher royalties that could be obtained without a RAND commitment. If a company has already made RAND commitments, it needs to investigate whether the encumbered patents are actually essential to the standard when facing litigation. Finally, the RAND commitment

310. *See generally* Maldonado, *supra* note 62; Contreras & Gilbert, *supra* note 63.

311. Contreras & Gilbert, *supra* note 63, at 31.

312. *See* Realtek Semiconductor Corp. v. LSI Corp., 946 F. Supp. 2d 998, 1008 (N.D. Cal. 2013).

313. *See* Microsoft Corp. v. Motorola, Inc., No. C10-1823JLR, 2013 WL 2111217, at *53–65 (W.D. Wash. Apr. 25, 2013).

314. *See* Contreras & Gilbert, *supra* note 63, at 31.

315. *See* Microsoft Corp. v. Motorola, Inc., 696 F.3d 872, 889 (9th Cir. 2012) (enjoining Motorola from enforcing a patent injunction against Microsoft in Germany); *see also Realtek*, 946 F. Supp. 2d at 1008 (filing a breach of contract claim before the International Trade Commission concluded its investigation or issued an exclusion order).

provides several defensive options for implementers under contract law. However, these options will only be available to implementers confronted with RAND-encumbered patents. While companies cannot choose the patents asserted against them, they can inquire as to whether the asserting party previously made a RAND commitment.

D. NEW PLAYS: NETWORK CROSS-LICENSING AGREEMENTS

Instead of relying on Congress—which is arguably in a worse state of gridlock than the patent system[316]—to provide further remedies, practitioners have continued to develop new defensive plays to protect their interests. Recently, two network cross-licensing agreements[317] have been proposed as defensive options for practicing companies: the Defensive Patent License Agreement and the License on Transfer Agreement.

Companies may obtain cross-licenses similar to the provisions in the Defensive Patent License Agreement ("DPL") and License on Transfer Agreement ("LOT") with other companies through a series of bilateral agreements.[318] For example, Samsung and Cisco recently entered a cross-licensing agreement that included the two companies' existing patents as well as patents filed in the next ten years.[319] However, negotiating individual agreements with a large number of companies in the industry may be prohibitively expensive.[320]

Network cross-licensing agreements reduce transaction costs and enhance protection benefits through network effects. Network cross-licenses reduce transaction costs by eliminating the costs of negotiation between patent holders and providing a standard license with predictable terms for each participant.[321] Furthermore, the network cross-licensing agreements utilize positive network effects to enhance the benefits of

316. *See* Christopher Ingraham, *Congressional Gridlock Has Doubled Since the 1950s*, WASH. POST (May 28, 2014), http://www.washingtonpost.com/blogs/wonkblog/wp/2014/05/28/congressional-gridlock-has-doubled-since-the-1950s/.

317. In this Note, "network cross-licensing agreement" refers to any collective licensing agreement in which members grant reciprocal licenses to current or future patent rights.

318. Transaction costs could be reduced for companies seeking to obtain the licensing provisions contained in the LOT Agreement, but companies likely would negotiate on an individual basis for cross-licensing agreements more similar to the DPL Agreement.

319. *Cisco and Samsung Enter Into Patent Cross-License Agreement*, CISCO PRESS RELEASES (Feb. 5, 2014), http://newsroom.cisco.com/release/1342531/Cisco-and-Samsung-Enter-Into-Patent-Cross-License-Agree_2.

320. *See* Schultz & Urban, *supra* note 43, at 8.

321. *Id.* at 47.

participating.[322] As more companies join, the agreements provide more protection from litigation risks and become more attractive to new members.[323] While these benefits are common to both network cross-licensing agreements, the DPL and LOT Agreements contain distinct licensing provisions that lead to varying reductions in litigation exposure.

a) The Defensive Patent License (DPL) Network

The DPL Agreement, a standardized cross-license, "serves as the connection point for a distributed defensive cross-license network."[324] Upon joining the DPL network, a participant licenses its entire patent portfolio under a perpetual, worldwide, royalty-free license.[325] If a participant wants to stop offering its patents under the DPL, it may discontinue licensing to newcomers after six months' notice.[326] However, the participant may not revoke any licenses in place before the end of the notice period unless a licensee brings suit against another DPL participant offensively, in which case all DPL participants may suspend their licenses to the DPL party asserting its patents offensively.[327] Thus, upon entry to the DPL Agreement, companies grant other participants patent licenses that may only be revoked in specific situations. This structure provides protection to participants but requires more commitment than the LOT Agreement.

b) The License on Transfer (LOT) Agreement

Industry participants launched a networked, royalty-free cross-licensing agreement for transferred patents called the LOT Agreement.[328] LOT participants grant a license to other participants, but the license only becomes effective when patents transfer to non-participants.[329] Until transferred, participants preserve full use of their patents.[330] As an example, if a LOT participant owns one thousand patents and transfers two patents to a non-participant, the LOT Agreement grants all other

322. *Id.* at 23–24.

323. David L. Hayes & C. Eric Schulman, *A Response to a Proposal for a Defensive Patent License (DPL)* 5 (Feb. 4, 2013) (unpublished manuscript), *available at* http://ssrn.com/abstract=2054314.

324. Schultz & Urban, *supra* note 43, at 5.

325. *Id.* at 39.

326. *Id.* at 39–40.

327. *Id.*

328. *LOT Agreement*, GOOGLE PATENT PROGRAMS, http://www.google.com/patents/licensing/#tab=lot (last visited Jan. 18, 2015).

329. *Id.*

330. *Id.*

participants a license to the two transferred patents. Licenses to the other 998 patents remain untriggered.

The LOT Agreement allows for license termination when patents transfer to a "non-assertion entity."[331] For example, LOT Participant *A* transfers its patents to non-LOT Participant *B*, triggering the licensing provision. If LOT Participant *C* brings suit offensively against non-LOT Participant *B* and non-LOT Participant *B* qualifies as a "non-assertion entity" under the agreement, the license to LOT Participant *C* may be terminated so that non-LOT Participant *B* can use the transferred patents defensively.

c) Reduction in Litigation Exposure: Protection from NPE use of Defensively Aggregated Patents

These network cross-licensing agreements protect companies from multiple litigation threats. As discussed, NPEs obtain defensively aggregated patents through two monetization strategies implemented by practicing companies: direct sale of patents to NPEs or patent privateering arrangements. If a company sells patents to NPEs, it typically includes a grant-back license to eliminate the risk of the patents being used against them after the sale.[332] Unlike the typical grant-back provision that only prohibits NPEs from asserting against the seller, the DPL and LOT Agreements prohibit NPEs from asserting transferred patents against all licensed participants. Under the DPL, each participant grants other participants a perpetual license upon joining the DPL.[333] LOT participants grant licenses to other participants that become effective when patents are transferred to non-participants.[334] Thus, both agreements reduce the number of potential targets for NPEs and consequently diminish the profits NPEs derive from purchasing encumbered patents.

In addition, companies indirectly monetize patents by transferring rights to NPEs through privateering arrangements.[335] The structure of the LOT Agreement targets this practice. Because the license does not trigger unless a patent transfers to a non-participant,[336] LOT allows practicing companies to bring suit directly against other participants and confront the risk of retaliation and reputational damage. However, companies cannot

331. LOT Agreement § 1.1(c) *available at* http://www.lotnet.com/how-to-join-lotnet/index.cfm (last visited Jan. 18, 2015).

332. Fawcett & Chan, *supra* note 231, at 20.

333. Schultz & Urban, *supra* note 43, at 39.

334. *LOT Agreement*, *supra* note 328.

335. *See* Ewing, *supra* note 221 at 8–9.

336. LOT Agreement § 1.1(c), *supra* note 331.

avoid these risks by transferring their patents to NPEs under privateering arrangements because the LOT license triggers upon transfer. The LOT Agreement deters companies from entering into privateering arrangements with NPEs and decreases the value of encumbered patents to NPEs. The DPL Agreement also protects participants against privateering because the agreement grants participants a license upon entry. Just as countries in the 1800s abolished privateering through treaties,[337] companies eradicate detrimental patent privateering against other participants when they sign the LOT or DPL Agreements. Although both agreements eliminate the threat of patents transferred by participants, companies face additional litigation exposure.

d) Reduction in Litigation Exposure: Protection from Direct Assertion by Practicing Companies

When the patent system functions as intended, companies use patent rights as a tool to recoup the costs of developing a new technology by allowing the patent holder to prohibit other companies from making, using, selling, or importing the patented technology.[338] Under the LOT Agreement, participants may still assert their patents against LOT participants and non-participants in this manner because the license does not trigger unless a patent transfers to a non-participant.[339] Thus, nothing in the LOT Agreement prevents companies from asserting their patents, but the companies must face the risk of retaliation and reputational damage.

Under the DPL Agreement, participants forfeit their ability to assert patents against other participants.[340] While the DPL limits companies' abilities to assert their patents, it also eliminates the risk of suit from other participating companies. This protection could create more freedom to operate with respect to DPL technologies,[341] allowing participating companies to compete on the merits of their products or services—rather than competing in the courtroom.[342] Furthermore, the DPL Agreement does not prohibit participants from asserting their patents against non-participants.

337. Ewing, *supra* note 221, at 8.
338. *See* Lemley, *supra* note 4, at 129–30.
339. LOT Agreement § 1.1(c), *supra* note 331.
340. *See* Schultz & Urban, *supra* note 43, at 39–40.
341. *See id.* at 48.
342. *See* Hayes & Schulman, *supra* note 323, at 4–5.

e) Litigation Exposure: Incomplete Protection

However, neither the DPL Agreement nor the LOT Agreement will protect companies from patents already owned by NPEs or obtained by NPEs from non-participants.

f) Network Cross-Licensing Agreement Limitations

Furthermore, network cross-licensing agreements impose some limitations in order to provide the positive attributes previously discussed. Network cross-licensing agreements inevitably lower the value of participants' patents because the patents no longer provide an exclusive right.[343] The license granted to other participants restricts a purchaser's ability to bring suit, so the value of the patent decreases.[344] This reduction in value may be a deterrent for both large portfolio companies and startup companies. Large portfolio companies lose significant monetary value in their assets by encumbering their patents with licenses, and startup companies hinder their ability to sell off patents as a method of mitigating losses upon failure.

Because their licensing provisions differ, the DPL and LOT Agreements contain additional, distinct limitations.

i) DPL Agreement Limitations

The risk and limitations of the DPL may deter companies from participating. First, even the creators of the DPL recognize that the DPL is not a viable option for companies with business models dependent upon monetization of their patent portfolios.[345] Companies that actively enforce and rely on patents to recoup investments may instead consider the LOT Agreement, which allows direct assertion of patents.

Second, large portfolio companies may not join the DPL because of the potential for disproportionate benefits.[346] A company with a minimal patent portfolio may benefit significantly more than companies that have spent substantial money aggregating large patent portfolios.[347] A company with few patents acquires licenses to all of the larger companies' aggregated patents without providing much benefit in return.[348] Further, a small startup company could use the DPL as an opportunity to compete

343. *See id.* at 4–5.
344. *See id.* at 5.
345. *See* Schultz & Urban, *supra* note 43, at 52.
346. Hayes & Schulman, *supra* note 323, at 5–6.
347. *Id.*
348. *Id.*

with large portfolio companies without the risk of patent infringement.[349] Later, when the startup company reaches a position where it is strong enough to survive patent litigation, it could simply terminate its status as a DPL participant.[350]

Lastly, the biggest deterrent to the DPL may be the risk associated with joining. Once a company joins the DPL, the license granted becomes irrevocable unless another member of the DPL offensively attacks.[351] Therefore, companies must be so confident in the value of joining the DPL that they will risk their entire existing patent portfolio, which may have cost millions of dollars to aggregate.

ii) LOT Agreement Limitations

The LOT Agreement faces fewer deterrents to entry for companies but provides less protection from litigation. Unlike the DPL Agreement, the LOT Agreement allows participants to assert patents against other participants.[352] Depending on a company's monetization strategy, the LOT structure could be viewed as a limitation or a benefit. If a company's patent portfolio consists of patents that will not be asserted, the company may view the lack of protection from other participants' patents as a limitation.[353] On the other hand, companies that seek to enforce their patents may not view this as a limitation because the freedom of assertion may outweigh the lack of protection.[354]

The LOT Agreement does not face the same lopsided benefit limitation present in the DPL Agreement. The LOT Agreement does not appear to favor companies with large patent portfolios or minimal portfolios. Due to the sheer number of aggregated patents, companies with larger portfolios provide substantial benefit to minimal portfolio companies by providing a larger number of licenses to minimal portfolio companies if the aggregated patents are later transferred to NPEs. Similarly, the LOT Agreements provide large companies significant protection against patents transferred by failed startups to NPEs.

The reduction in participants' exposure increases as more operating companies join the LOT network.[355] Therefore, the success of the LOT

349. *Id.*
350. *Id.*
351. *Id.*
352. *LOT Agreement*, *supra* note 328.
353. These companies likely would be better suited with the DPL Agreement.
354. *See* Hayes & Schulman, *supra* note 323, at 27.
355. *Id.* at 27.

Agreement depends on whether the LOT Agreement can utilize positive network effects to incentivize other companies to join. Google, Canon, SAP, Newegg, Dropbox, and Asana joined the LOT network and placed 300,000 patents into the LOT pool.[356] It is unclear whether these patents will provide sufficient incentive for others to join.

g) Summary of the DPL and LOT Plays

Strategically, until the DPL has significant participation, companies with larger patent portfolios may individually cross-license with other companies to avoid the potential lopsided benefits and risks of joining the DPL. Companies with minimal patent portfolios and infrequent monetization may join the DPL for the added protection and terminate participation if their patent strategy or position begins to shift.[357]

The LOT Agreement provides less protection than the DPL but requires less commitment. While the LOT Agreement imposes some limitations for companies seeking to monetize patents through direct sale or patent privateering, it provides diminished risk because all patents remain unencumbered until transferred. Companies with large defensive portfolios and startup companies should consider the LOT Agreement if the value gained outweighs the ability to monetize their portfolio by collaborating with NPEs.

IV. DEVELOPING DEFENSIVE PLAYS

Currently, two additional developments may provide future defensive options: inter partes reviews and enhanced fee-shifting. These areas of the law have not fully developed, but this Part introduces these evolving defenses.

Companies may utilize inter partes reviews ("IPRs") to invalidate asserted patents. During an IPR, the Patent Trial and Appeal Board ("PTAB") will evaluate patentability "under section 102 or 103 . . . on the basis of prior art consisting of patents and printed publications"[358] if the requesting petitioner demonstrates "a reasonable likelihood" that the PTAB would find at least one claim invalid.[359] If the petitioner requests an

356. *Asana, Canon, Dropbox, Google, Newegg and SAP Announce Formation of New Cooperative Patent-Licensing Agreement*, CANON GLOBAL (July 10, 2014), http://www.canon.com/news/2014/jul10e.html.

357. *See* Hayes & Schulman, *supra* note 323, at 5–6.

358. 35 U.S.C. § 311(b) (2012).

359. 35 U.S.C. § 314(a) (2012).

IPR after the commencement of patent litigation, a district court will often stay the case.[360]

Effectively, a stay offers litigants a choice between arguing validity in district courts or at the PTO. District courts construe claims according to "the meaning that [a] term would have to a person of ordinary skill in the art in question at the time of the invention."[361] However, during IPRs, the PTAB uses the "broadest reasonable construction in light of the specification of the patent in which it appears."[362] Additionally, the burden of proof differs. A district court requires clear and convincing evidence to invalidate a patent claim, but the PTAB requires only a preponderance of evidence to invalidate a patent claim.[363] Early IPR decisions by the PTAB indicate that the PTO may be a favorable forum for patent challengers,[364] but companies need to monitor the challenger success rate and analyze a larger sample size before reaching such a conclusion.

In addition to the AIA developments, a recent Supreme Court decision indicates that fee-shifting might become a more serious threat to NPEs moving forward. Under 35 U.S.C. § 285, a court may only award attorney fees to the prevailing party in "exceptional cases."[365] In *Octane Fitness, LLC v. ICON Health & Fitness, Inc.*, the Court articulated a more discretionary standard for determining whether a case is "exceptional."[366] This discretionary standard could mitigate the current asymmetrical exposure present in patent litigation and gives practicing entities a greater threat against NPEs.[367]

360. Jason E. Stach & Jeffrey A. Freeman, *District Court or the PTO: Choosing Where to Litigate Patent Invalidity*, FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP IP LITIGATOR (Mar./Apr. 2014), http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=e7ad4528-cec4-4889-a23d-d17bca527ca2.

361. Phillips v. AWH Corp., 415 F.3d 1303, 1313 (Fed. Cir. 2005).

362. 37 C.F.R. § 42.100(b) (2013).

363. 35 U.S.C. § 316(e) (2012).

364. David Cavanaugh, *Early Results of Post Grant Proceedings*, INTELL. PROP. TODAY (July 31, 2014), http://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/IP-today-early-results-post-grant-proceedings-July-2014.pdf (evaluating IPR decisions from September 16, 2012 until May 1, 2014).

365. 35 U.S.C. § 285 (2012).

366. *Octane*, 134 S. Ct. at 1749.

367. *See* Hannah Jiam, Note, *Fee-Shifting and* Octane Fitness*: An Empirical Approach Towards "Exceptional"*, 30 BERKELEY TECH. L.J. 611 (2015).

V. CONCLUSION

The patent system is a complex puzzle that constantly evolves. Multiple factors have contributed to the current patent landscape. First, in the 1980s, the Federal Circuit situated the patent system for rapid growth. With the patent system primed for growth, licensing and assertion campaigns catalyzed a patent aggregation "arms race" that increased patent filings and resulted in webs of overlapping patent rights.[368] Subsequently, after the dot-com bubble burst, NPEs obtained many of these patents and became prominent players in the patent field by exploiting asymmetrical costs and risks. As a result, the current landscape faces the accumulation of these obstacles and an increasing transition from patent aggregation to patent monetization.

These eras produced numerous defensive strategies to help companies compete in the patent landscape: defensive aggregation, RAND cross-licensing, open source licenses, lobbying for doctrinal changes, public disclosure, patent pledges, third-party defensive protection, and network cross-licensing agreements. These defensive plays range from general strategies to specific litigation tactics.

The evolution of the defensive patent playbook will continue as companies develop new strategic maneuvers, new players emerge in the patent field, and courts define the contours of the AIA. No single private action will cure the current patent system. The viability of these "plays" will be dictated by each individual company's patent portfolio, business goals, and exposure to litigation. Ultimately, each option and strategy in the defensive patent playbook contains its own benefits, risks, and limitations that must be evaluated to prepare a successful patent game plan.

368. Chien, *From Arms Race to Marketplace*, *supra* note 5, at 304.

Chapter 23

Linux Defenders

LINUX DEFENDERS

About Linux Defenders

Our mission is to educate and empower the Free and Open Source Software community around the expensive and litigious minefield that comprises the modern software patent landscape.
Read More >>

Educational Resources

We provide information on defensive intellectual property strategies for the Free and Open Source software community, to help combat patent aggressors.
Read More >>

Defensive Publications

We encourage the creation of defensive publications to block others from receiving future patents on inventions that have already been documented in a defensive publication from the Free and Open Source Software community.
Read More >>

Prior Art Activities

We review past and present patents that threaten the Free and Open Source software community and provide relevant, game-changing prior art whenever possible.
Read More >>

Sponsors and Affiliates

THE LINUX FOUNDATION

Software Freedom Law Center

openinventionnetwork

Linux Defenders
Research Triangle Park Center
4819 Emperor Blvd., Suite 400
Durham, NC 27703

info@linuxdefenders.org

P +1 919.313.4902
F +1 919.313.4905

Chapter 24

Microsoft Expands Its Patent Protection Program to Include Azure-powered IoT Devices (Mary Jo Foley)

Microsoft expands its patent protection program to include Azure-powered IoT devices

Microsoft is extending its Azure IP Advantage patent-protection program into the IoT space to help its customers fight patent trolls.

By Mary Jo Foley for All About Microsoft | | Topic: Internet of Things

Microsoft is expanding its Azure IP Advantage patent-protection program to cover IoT devices connected to Azure. The company also is donating 500 patents to the LOT Network that are targeted specifically at startups.

Microsoft announced its new patent-program extensions, as well as a number of other IoT-focused product updates on March 28, a week ahead of the Hanover Messe industrial manufacturing show in Germany.

Microsoft originally took the wraps off Azure IP Advantage in February 2017. At that time, Microsoft officials said they would make 10,000 Microsoft patents available to Azure customers to help them defend themselves against "baseless patent lawsuits." All Azure customers are automatically covered by Azure IP Advantage.

Today, Microsoft execs said that Azure IP Advantage also will now cover all Azure customers with IoT devices connected to Azure; devices powered by its Azure Sphere microcontroller solution; and Windows IoT.

In October 2018, Microsoft joined the LOT Network as another step intended to try to help fight patent trolls. The LOT Network is a nonprofit community working to fight trolls. The group has nearly 300 members, covering approximately 1.35 million patents, Microsoft officials said.

LOT Members are free to cross-license, assert, sell or do nothing with their patents. But if any member of the LOT Network sells a patent to a troll, all LOT members automatically get a free license to that patent. Microsoft officials said today they now donating 500 patents to LOT that are specifically for startups. Here's how startups can qualify for those.

Microsoft execs also announced today that Azure Sentinel, its new security information and event management (SIEM) service also now covers IoT devices. And Azure IoT Hub now integrates with Azure Security Center directly.

https://www.zdnet.com/article/microsoft-expands-its-patent-protection-program-to-include-azure-powered-iot-devices/

Chapter 25

GNOME Foundation Facing Lawsuit from Rothschild Patent Imaging

News (https://www.gnome.org/news/)

September 25, 2019

GNOME Foundation facing lawsuit from Rothschild Patent Imaging

The GNOME Foundation has been made aware of a lawsuit (https://insight.rpxcorp.com/litigation_documents/13472237) from Rothschild Patent Imaging, LLC over patent 9,936,086 (https://patents.google.com/patent/US9936086B2/en). Rothschild allege that Shotwell (https://wiki.gnome.org/Apps/Shotwell), a free and open source personal photo manager infringes this patent.

Neil McGovern, Executive Director for the GNOME Foundation says "We have retained legal counsel and intend to vigorously defend against this baseless suit. Due to the ongoing litigation, we unfortunately cannot make any further comments at this time."

Updates to this case will be published on www.gnome.org (https://www.gnome.org).

Read the archives... (https://www.gnome.org/news/)

Part V

FOSS in Asia

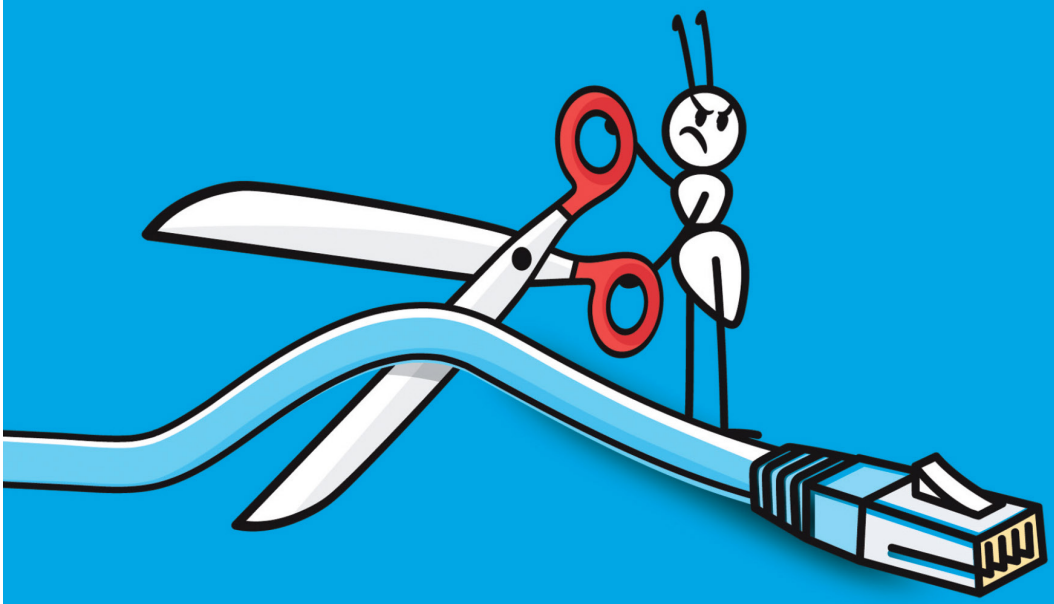
Chapter 26

Living in Darkness: Guide to Internet Shutdowns in India (sflc.in)

sflc.in

Living in Digital Darkness

A Handbook on Internet Shutdowns in India



May 2018

Living in Digital Darkness: A Handbook on Internet Shutdowns in India

Published by: SFLC.in

SFLC.in
K9, 2nd Floor, Birbal Road
Jangpura Extension
New Delhi – 14
India

Email: mail@sflc.in
Website: https://www.sflc.in
Twitter: @SFLCin

Table of contents

List of abbreviations

CEO	*Chief Executive Officer*
CrPC	*Code of Criminal Procedure*
GDP	*Gross Domestic Product*
ICT	*Information and Communication Technologies*
IPC	*Indian Penal Code*
ISP	*Internet Service Provider*
IT	*Information Technology*
RTI	*Right to Information*
SMS	*Short Message Service*
Telecom	*Telecommunications*
TSP	*Telecommunications Service Provider*
UN	*United Nations*
UNHRC	*United Nations Human Rights Council*
VSAT	*Very Small Aperture Terminal*
WSIS	*World Summit on the Information Society*

List of statutes

- Code of Criminal Procedure Code, 1973
- Indian Penal Code, 1860
- Indian Telegraph Act, 1885
- Temporary Suspension of Telecom Services, (Public Emergency or Public Safety) Rules, 2017
- Information Technology Act, 2000
- Right to Information Act, 2005

CHAPTER 1

Introduction

The Internet has long been identified as one of the greatest technological advancements of recent times, and has proven over the years to be a critical enabler of social and economic change. As observed by the Outcome Document of the High-Level Meeting of the United Nations General Assembly on the Overall Review of the Implementation of WSIS Outcomes, Information and Communication Technologies (ICTs) including the Internet have seen penetration into almost all corners of the globe, created new opportunities for social interaction, enabled new business models, and contributed to economic growth and development in all other sectors. It was further observed that increased ICT connectivity, innovation, and access have played a critical role in enabling progress on the Millennium Development Goals.

"Governments across the world are increasingly resorting to Internet shutdowns (also referred to as Internet blackouts) for a wide range of reasons, all with the objective of controlling the exchange of information online."

However, Governments across the world are increasingly resorting to Internet shutdowns (also referred to as Internet blackouts) for a wide range of reasons, all with the objective of controlling the exchange of information online. The most widely cited reason for instituting Internet shutdowns is that law and order breakdowns are made worse by rumors and misinformation circulating online, and curbing access to the Internet is an effective aid in restoring normalcy. During a shutdown, Government agencies usually order Telecom Service Providers (TSPs) to stop providing Internet services in one or more localities so that residents are prevented from easily accessing and circulating information that is seen as incendiary or otherwise harmful.

The frequent resort to Internet shutdowns by the State as a mitigation and prevention strategy, mostly in the developing countries is a cause of concern. Between January 2012 and May 1, 2018, India has experienced 174 Internet shutdowns for various reasons and durations across 19 of the 29 states in the country[1]. Apart from India, Internet shutdowns have also been reported in over 30 other countries, including among others, Pakistan, Bangladesh, Mynamar, Egypt, Congo, Syria, Sudan, Burundi, Iraq, and Venezuela.

Frequent Internet shutdowns by the State come with several problems, like obstructing the free flow of information and essentially bringing many aspects of modern society to a grinding halt. Businesses, educational institutions, hospitals, and even Governments themselves have come to rely extensively on the Internet over time, and without it, the day-to-day functioning of such entities are significantly crippled. It has also been argued that cutting off

1. Internet Shutdown Tracker, available at: https://www.internetshutdowns.in, last accessed on May 1, 2018

Internet access in a crisis prone/inflicted area might prove to be detrimental rather than beneficial, as a disconnect from the Internet in such situations restricts the accurate and timely reportage that is necessary even for relief and disaster management.

It is troubling that even though the world has taken collective cognizance of the importance of the Internet in enabling sustainable growth and development, and most jurisdictions have laws that guarantee and ensure respect for fundamental human rights such as the right to free speech and expression, Internet shutdowns are nevertheless gaining momentum in many parts of the world. Not only do Internet shutdowns disrupt the smooth functioning of societies, but they also make human rights a hostage to the whims of Governments. Specially in the absence of laws that demand a particular standard of scrutiny and transparency, Internet shutdowns pose serious threats to development and perhaps democracy itself.

Scope

This report seeks to provide a detailed look at how Internet shutdowns work in India so as to add to the growing body of research literature that informs policy discussions in this regard. To this end, it will briefly go over how Internet shutdowns have surfaced and grown in the country, analyze the laws and policies that govern their imposition, provide a glimpse into how Internet shutdowns may cause real-world problems in the long and short run, and take stock of the efforts that have gone into defining and addressing Internet shutdowns as a public policy issue. We hope that this report will prove useful to everyone who wishes to actively or passively participate in the debate around Internet shutdowns on any level. As the Internet stakeholder community comprises virtually all Internet users, this includes everyone from daily consumers of online infotainment, to students, researchers, and academicians who rely on the Internet to a large extent for research, businesses that have migrated much of their day-to-day operations online, civil society members looking to effectively engage in policy discussions, and even the Government, who has the unenviable task of regulating the open Internet in a fair, just, and reasonable manner while making sure that it is not used in ways that threaten the safety and well-being of citizens.

Methodology

A mix of primary and secondary research has been used in drafting this report. Existing literature on the topic such as books, reports, news articles, blog posts and policy papers were consulted while drafting the explanatory sections of this report. All information on the reported instances of Internet shutdowns in India come from the dynamic Internet Shutdown Tracker we maintain at www.internetshutdowns.in, which in turn sources its data primarily from reports published in national and regional newspapers. Some information is also provided by residents from areas affected by Internet shutdowns using the "report a shutdown" feature that is made available to visitors of the website.

As such, we emphasize that the list of recorded Internet shutdowns in India must be approached with a certain amount of caution. We consider newspaper reports of Internet shutdowns to be more or less accurate by default, and therefore do not verify every report separately unless we have a reason to do so. On the

rare occasions when news reports present conflicting information on certain shutdowns for instance, we try our best to independently verify this information from primary sources such as residents from the affected areas. We also verify all information on Internet shutdowns that reaches us by word-of-mouth by soliciting corroborating reports from our sources. Only verified instances are added to our database in such cases. Even so, we advise that our record of shutdowns be treated as an indicative one, and not exhaustive.

CHAPTER 2

Understanding Internet shutdowns

What is an Internet shutdown?

We define an Internet shutdown as "a Government-imposed disablement of access to the Internet as a whole within one or more localities for any duration of time". There are two key-components to this definition:

1. An Internet shutdown is always Government-imposed i.e. Internet Service Providers serving the locality in question are ordered by an agency of the Government to cut-off Internet services to that area.

2. An Internet shutdown always imposes a blanket ban on Internet access, where access to the Internet as a whole is disabled, and not a selective ban, where access to particular content/services is disabled leaving access to other content/services unaffected.

It is pertinent to note that there is an extent of variability in how Internet shutdowns are defined by the global multi-stakeholder community. Some encapsulate instances of selective bans on Internet access within the meaning of the term "Internet shutdown", alongside blanket bans on access to the Internet as a whole. For instance, Access Now – an international non-profit organization that also spearheads the #KeepItOn campaign to end Internet shutdowns – defines an Internet shutdown as, *"an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information"*[2]. This definition notably excludes any references to the scope of disruption, which means selective bans may also be brought within its ambit.

It is argued at various policy forums that as the fundamental premise of both selective and blanket bans is about disabling access to online content/services, and as the former is an equally condemnable violation of human rights as the latter, there is no reason to view them as separate public policy issues. However, selective bans on Internet access are excluded from the scope of this report as it was felt that the emergence and rapid growth of blanket bans in India warrant treating them as a distinct issue. In addition, selective and blanket bans are built on separate legal foundations in India, and selective bans have rarely been imposed as responses to conflict situations owing to the ease with which they can be circumvented, and prevention/mitigation of conflict has become the primary reason to impose blanket Internet shutdowns in the country.

> "We define an Internet shutdown as "a Government-imposed disablement of access to the Internet as a whole within one or more localities for any duration of time"."

Unless specified otherwise, the term "Inter-

2. *What is an Internet Shutdown?*, available at: https://www.accessnow.org/keepiton/, last accessed May 1, 2018

net shutdown" as it appears in this report must be understood to refer to blanket bans on Internet access, and not selective bans.

Why are Internet shutdowns imposed?

In August 2012, residents hailing from North-Eastern India staged an exodus from the South Indian city of Bengaluru after rumors began to circulate on WhatsApp and various social media platforms that large-scale violence was being planned against them in the wake of ethnic clashes in the state of Assam(3). Even though no cases of actual violence seemingly took place in Bengaluru, residents from the North-East were reported as saying that there was an atmosphere of "fear and mistrust" in the city, fueled to a large extent by rumors of impending violence that were circulating online and offline(4). As a result, thousands rushed to the city's railway stations seeking to return to their hometowns, causing several stampede-like situations even after the Government announced two special trains on an emergency basis to accommodate the sudden influx of travelers. The city was thrown into chaos, leaving the authorities scrambling to contain the situation and prevent damage, injuries and loss of life. Moreover, the fact that this incident took place in Bengaluru, which had always been a relatively peaceful city and certainly not one known for incidents resulting from ethnic tensions, drove some to speculate that the panic was engineered through one or more systematic campaigns to create fear using social media, SMS and regional media(5). The speculations were based largely on the fact that none interviewed by the media were able to cite even a single incident of actual violence in the city, and appeared to be acting mostly on rumors circulating online and offline.

Whatever the true reasons behind the uncharacteristic exodus from Bengaluru might have been, it was closely followed by the first instance of an Internet shutdown in India on September 21, 2012, when mobile Internet services were suspended for a few hours in the Kashmir Valley during protests against a movie that was deemed offensive to Islamic sentiments(6). This was the first time as per available information that mobile Internet services alone were suspended in India i.e. not as part of a broader telecommunications clampdown such as those imposed every Republic Day and Independence Day in the state of Jammu and Kashmir. The order issued in this regard by Jammu and Kashmir's Home Department does not reveal much information on reasons behind the shutdown, other than that it was imposed under Section 5(2) of the Indian Telegraph Act, 1885 *"in the interest of public safety and for maintaining public order"*(7). However, it can be inferred from the circumstances surrounding the shutdown as well as the language of the Home Department order that it was imposed to prevent further circulation of the movie "Innocence of Muslims", which was considered inflammatory and likely to cause violent protests. While reports were

3. Dipa Kurup, *After Rumors, Northeast People Flee Bangalore,* August 16, 2012, The Hindu, available at: http://www.thehindu.com/news/national/karnataka/after-rumours-northeast-people-flee-bangalore/article3776549.ece, last accessed on April 28, 2018

4. Ibid.

5. Lakshmi Chaudhry, *Mystery of the NE exodus: Why Bangalore?,* August 16, 2012, Firstpost, available at: https://www.firstpost.com/india/mystery-of-the-ne-exodus-why-bangalore-419876.html, last accessed on May 1, 2018

6. Pamposh Raina and Betwa Sharma, *Telecom Services Blocked to Curb Protests in Kashmir,* September 21, 2012, NY Times Blog, available at: https://india.blogs.nytimes.com/2012/09/21/telecom-services-blocked-to-curb-protests-in-kashmir/?_r=0, last accessed on April 28, 2018

7. Jammu and Kashmir Home Department Order No. Home – 811 of 2012, available at: http://jkhome.nic.in/7940001.pdf, last accessed on April 28, 2018

conflicted about whether this particular shutdown was a blanket ban on access or a selective ban, it nevertheless appears to be the first time an Internet shutdown was reported in any capacity by India's mainstream media.

Three more shutdowns were imposed in India in 2014, not counting the routine telecommunications clampdowns in Jammu and Kashmir on Republic Day and Independence Day[8]. All three shutdowns were imposed in various localities across Jammu and Kashmir after violence broke out during political and communal tensions. According to news reports, the shutdowns were imposed as a measure to contain outbreaks of violence by limiting the spread of rumors and misinformation online. In fact, every Internet shutdown that has been imposed since September 21, 2012 until April 30, 2018 save a negligible few, was imposed either as a measure to prevent violence when violence was considered likely or as a measure to contain the spread of violence after violence had already broken out.

It would appear that the North-East exodus from Bangalore (and possibly numerous smaller-scale, less widely reported incidents before it) had demonstrated to law enforcement authorities and others in the Government that the Internet can act as a powerful tool for those seeking to disrupt law and order for any reason. As invaluable as the Internet is in enabling sustainable growth and development, the authorities had seen first-hand that it is also vulnerable to exploitation by those with malicious intent. Services like WhatsApp, Facebook, Twitter, and others allow virtually anyone to create and broadcast content designed to inspire fear and instigate chaos. In addition, they make it easier for the perpetrators to organize themselves and plan out their disruptions in careful detail. Law enforcement agents also have a more difficult time apprehending the perpetrators who often have the added advantage of encryption protocols covering their digital footprints.

"It would appear that the North-East exodus from Bangalore (and possibly numerous smaler-scale, less widely reported incidents before it) had demonstrated to law enforcement authorities and others in the Government that the Internet can act as a powerful tool for those seeking to disrupt law and order for any reason."

When faced with an imminent or existing law and order breakdown, Internet shutdowns have gradually become a popular component of the wider array of State responses like curfews, media clampdowns and others. It is firmly believed by state agencies that such a blanket shutdown would completely stop the spread of rumors and misinformation online, and by extension, any escalations in panic or violence that may otherwise have taken place. While selective bans on Internet access i.e. access to popular communication and social networking platforms like WhatsApp, Facebook, Twitter and YouTube have also been imposed during law and order situations in the past, blanket Internet shutdowns are heavily favored by the State as selective bans are relatively easy to circumvent using workarounds like Virtual Private Networks and proxy servers. Instructing TSPs to cut off access to the entire Internet

8. Supra. 1 on May 1, 2018

effectively solves this problem, and ensures that Internet shutdowns function as they are expected to. Problems caused by blanket shutdowns like disruptions in e-commerce, e-banking and e-governance among many others are seen as permissible collateral damage during public emergencies.

There are three primary legislations under which Internet shutdowns are imposed in India – these are (1) Section 144 of the Criminal Procedure Code, 1973; (2) Section 5(2) of the Indian Telegraph Act, 1885; and (3) the Temporary Suspension of Telecom Services (Public Emergency and Public Safety) Rules, 2017. The next section of this report will examine how these legislations tackle Internet shutdowns, and how they are used to curb Internet access at various points.

CHAPTER 3

Internet shutdowns under law

When it comes to understanding existing legal mechanism for internet shutdowns in India, there are two statutes and a set of rules i.e Code of Criminal Procedure 1973 (CrPC), Indian Telegraph Act 1885, and Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 (hereinafter, the Telecom Suspension Rules), which confer powers upon Government agencies to order blanket network outages in districts and states of India.

Section 144, Code of Criminal Procedure, 1973

A vast majority of Internet shutdowns recorded in India between January 2012 and April 2018 have been ordered under Section 144 of the CrPC, 1973. Concrete statistics on the number of invocations is unavailable as news reports often do not mention the provision under which shutdowns were imposed, but it can safely be said from available reports that this provision was heavily favored at least until the Telecom Suspension Rules were notified in 2017, though it has continued to be intermittently used even afterwards.

“A vast majority of Internet shutdowns recorded in India between January 2012 and April 2018 have been ordered under Section 144 of the CrPC, 1973”

The CrPC is a collection of procedural laws that govern how substantive criminal laws enumerated under the Indian Penal Code, 1860 are to be enforced and covers such aspects as investigation and prosecution of offences among others. Within the CrPC, Section 144 resides as the sole occupant under the chapter of “temporary measures to maintain public tranquility” and gives State Governments the “power to issue orders for immediate remedy in urgent cases of nuisance or apprehended danger”.

From a bare reading, the core aspects of Section 144 that are relevant when discussing Internet shutdowns can be broken down as follows:

- The authority to issue orders under this Section lies with the District Magistrate, a sub divisional magistrate or any other Executive magistrate specially empowered by the State Government in this behalf.

- Before an order can be issued under Section 144, the issuing authority must be satisfied that there is sufficient ground for proceeding under this Section, and that immediate prevention or speedy remedy is desirable.

- Any order issued under Section 144 must be in writing, stating the material facts of the case and served in accordance to applicable legal procedure.

- The order so issued and served can “direct any person to do or abstain from a certain act” or “to take certain order with respect to certain property in his possession or under his management”. In other words, the order can ask anyone to do or not do anything, or to perform a specific action as directed with respect to any property they possess or manage.

• In the issuing authority's view, the order must be "likely to prevent, or tends to prevent, obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquillity, or a riot or an affray".

Section 144 was a provision designed to help contain law and order situations by vesting State Government officials with emergency powers, and it has traditionally been used to issue curfews and dismiss unlawful assemblies during widespread civil unrest. The Section accordingly features broad language that is necessary to allow issuing authorities to carry out their duties effectively, and does not contain any checks and balances to prevent abuse other than limiting the maximum duration of orders to 6 months and empowering third-party State Government officials to rescind orders issued by another.

In context of Internet shutdowns, Section 144 implies that a District or Sub Divisional Magistrate can order TSPs to stop providing Internet services within the Magistrate's jurisdiction (as the network architecture is a property under the TSPs possession and management), if it is felt that doing so would prevent law and order situations from arising or escalating. It must be noted words such as "obstruction, annoyance, disturbance to public tranquillity or an affray" are not defined under the CrPC or any other legislation, thus opening the statutory provision to heterogeneous interpretations.

As an archaic provision of law that has been carried down from the British Raj, this Section was clearly not designed to oversee State actions like Internet shutdowns, where a lot more nuances must ideally be considered before imposing restrictions. A District Magistrate speaking on Internet shutdowns at an event expressed that he prefers imposing shutdowns under Section 144 as the process is less cumbersome when compared to other legislations[9]. The orders to invoke Section 144 in online scenario for internet world are far-fetched because they prevent the public at large from accessing and using internet for any purpose including areas like like education and business.

"As an archaic provision of law that has been carried down from the British Raj, this Section was clearly not designed to oversee State actions like Internet shutdowns, where a lot more nuances must ideally be considered before imposing restrictions."

9. *Report Launch by ICRIER, "Internet Blackout: Measuring the Economic Blackout of Internet Shutdowns in India"*, See: https://sflc.in/report-launch-icrier-internet-blackout-measuring-economic-blackout-internet-shutdowns-india, last accessed on May 1, 2018

ORDER UNDER SECTION 144 OF THE CODE OF CRIMINAL PROCEDURE 1973

Whereas it has been made to appear before me that the Jat reservation agitation has spread throughout the District Hisar. There are ongoing instances and further likelihood of blockade of Railway track, highway and other roads by the agitators. Similarly, there is likelihood of damage to public property and commission of cognizable offences related to safety and security of individuals and property. This has caused a great inconvenience to the general public and adversely affected the essential services and supply of commodities. Many gatherings of these agitators are being facilitated by way of spreading disinformation and rumours through various social media such as Whatsapp, Facebook, Twitter, Instagram, Flickr, Tumblr, Google+, on mobile phones. Similarly, SMS services on mobile phones are being used to spread disinformation and for facilitating gatherings of agitators. As per reports received, there is imminent danger of disturbance of public tranquility due to inflammatory material being transmitted/ circulated to the public through social media/ messaging services on internet 2G/3G/Edge/ GPRS.

In view of the tense situation in Haryana and on account of Law & Order disturbance, I, Dr. Chander Shekhar Khare, District Magistrate Hisar, by virtue of powers conferred under section 144 of the Code of Criminal Procedure, 1973, hereby order immediate stoppage the internet services (2G Edge, 3G, 4G, GPRS) provided on mobile network in the territorial jurisdiction of Hisar District, Haryana. Telecom Service Providers are hereby directed to ensure compliance of this order.

This order is issued to prevent any disturbance of peace and public order in the jurisdiction of Haryana and shall remain in effect till further orders.

This Order is being passed ex-parte in view of the emergent situation.

In case of violation of the aforesaid order, person found guilty shall be liable to be punished as per Section 188 of the Indian Penal Code.

Given under my hand and the seal of the court this day, 18th February 2016.

District Magistrate
Hisar.

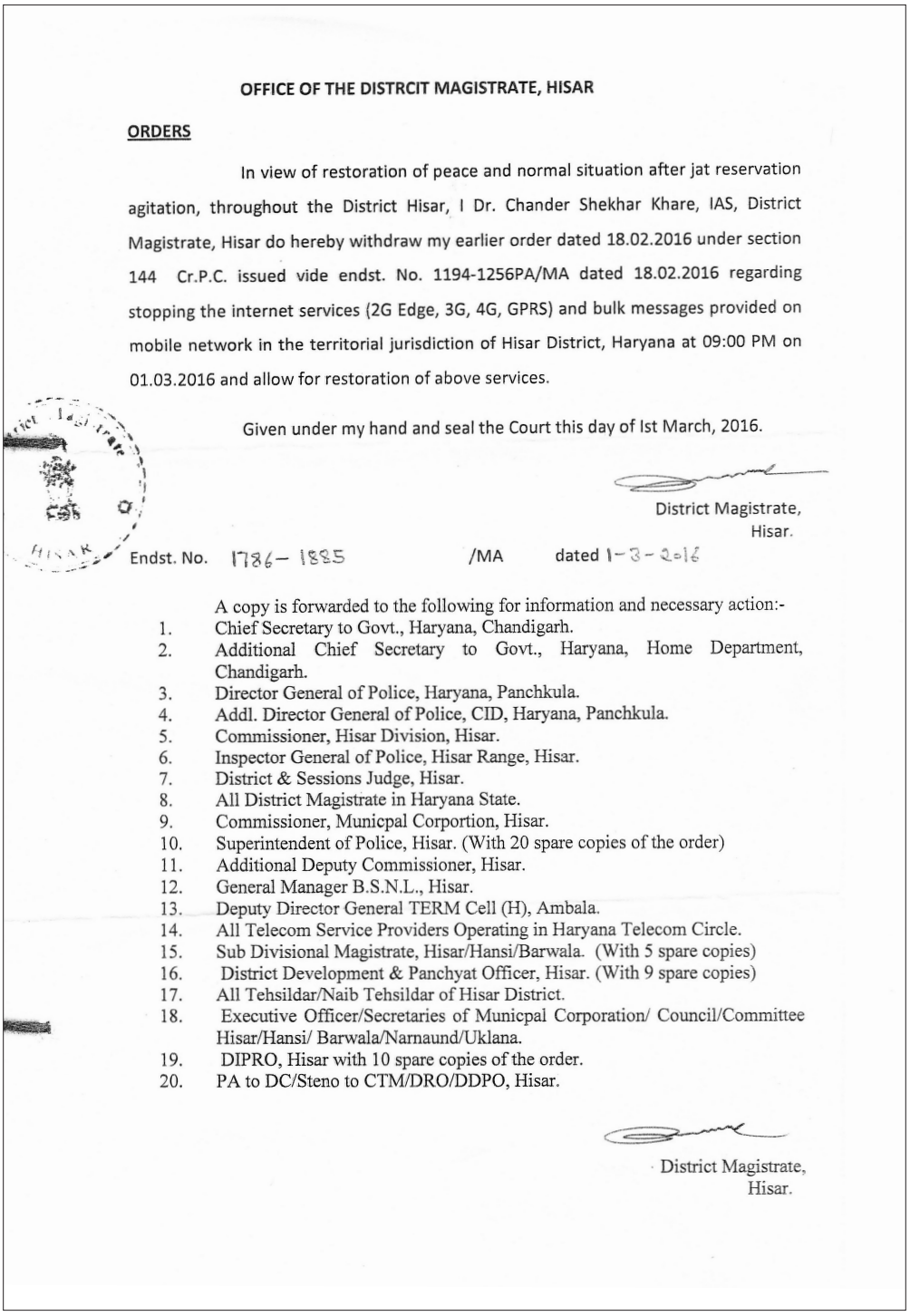
No. 1194-1256 /PA(MA , dated 18/02/2016

A copy of the above is forwarded to the following for information and necessary action please:-

1. The Deputy Director General, TERM Cell (H), Ambala.
2. All Telecom Service Providers operating in Haryana Telecom Circle.
3. The Chief Secretary to Govt. Haryana. (For information)
4. The Addl. Chief Secretary to Govt. Haryana, Home Department, Chandigarh. (For information)
5. The Director General of Police, Haryana, Panchkula. (For information)
6. The Addl. Director General of Police, CID (H) Panchkula. (For information)
7. Divisional Commissioner, Hisar .
8. District & Session Judge, Hisar.
9. All District Magistrates in the state.
10. The Superintendent of Police Hisar with 5 spare copies
11. SDM Hisar/Hansi/Barwala.
12. CTM Hisar.
13. Civil Surgeon Hisar.
14. All Tehsildars/Naib Tehsildars in District Hisar.
15. All BDPOs in District Hisar.
16. DIPRO Hisar.
17. PA to DM Hisar.

District Magistrate,
Hisar

(Example of Internet shutdown order issued under Section 144, CrPC, obtained under RTI Act)



OFFICE OF THE DISTRCIT MAGISTRATE, HISAR

ORDERS

In view of restoration of peace and normal situation after jat reservation agitation, throughout the District Hisar, I Dr. Chander Shekhar Khare, IAS, District Magistrate, Hisar do hereby withdraw my earlier order dated 18.02.2016 under section 144 Cr.P.C. issued vide endst. No. 1194-1256PA/MA dated 18.02.2016 regarding stopping the internet services (2G Edge, 3G, 4G, GPRS) and bulk messages provided on mobile network in the territorial jurisdiction of Hisar District, Haryana at 09:00 PM on 01.03.2016 and allow for restoration of above services.

Given under my hand and seal the Court this day of Ist March, 2016.

District Magistrate,
Hisar.

Endst. No. 1786– 1885 /MA dated 1-3-2016

A copy is forwarded to the following for information and necessary action:-

1. Chief Secretary to Govt., Haryana, Chandigarh.
2. Additional Chief Secretary to Govt., Haryana, Home Department, Chandigarh.
3. Director General of Police, Haryana, Panchkula.
4. Addl. Director General of Police, CID, Haryana, Panchkula.
5. Commissioner, Hisar Division, Hisar.
6. Inspector General of Police, Hisar Range, Hisar.
7. District & Sessions Judge, Hisar.
8. All District Magistrate in Haryana State.
9. Commissioner, Municpal Corportion, Hisar.
10. Superintendent of Police, Hisar. (With 20 spare copies of the order)
11. Additional Deputy Commissioner, Hisar.
12. General Manager B.S.N.L., Hisar.
13. Deputy Director General TERM Cell (H), Ambala.
14. All Telecom Service Providers Operating in Haryana Telecom Circle.
15. Sub Divisional Magistrate, Hisar/Hansi/Barwala. (With 5 spare copies)
16. District Development & Panchyat Officer, Hisar. (With 9 spare copies)
17. All Tehsildar/Naib Tehsildar of Hisar District.
18. Executive Officer/Secretaries of Municpal Corporation/ Council/Committee Hisar/Hansi/ Barwala/Narnaund/Uklana.
19. DIPRO, Hisar with 10 spare copies of the order.
20. PA to DC/Steno to CTM/DRO/DDPO, Hisar.

District Magistrate,
Hisar.

(Example of Internet restoration order issued under Section 144, CrPC, obtained under RTI Act)

The practice of invoking Section 144 to impose Internet shutdowns was in fact challenged at the Gujarat High Court as a Public Interest Litigation (PIL) in *Gaurav Sureshbhai Vyas v. State of Gujarat* [W.P. (PIL) No. 191 of 2015]. It was argued that the power to block certain information on an online/ computer related forum was given in Section 69A of the Information Technology Act, 2005 hence the State Government was not competent to use Section 144 CrPC to restrict the use of Internet. While delivering the judgment for the case challenging the authority behind shut down of mobile Internet in Gujarat, the Gujarat High Court defended the State Government's authority under Section 144 CrPC. It held that the state government is a competent authority under this provision and it depends upon their discretion to exercise the power with prudence, public duty and the sufficiency of action in their view[10]. Furthermore, the court refrained from exercising appellate power to decide upon the 'sufficiency of matter to exercise power under Section 144.' It limited its decision to the question of whether there was an 'arbitrary exercise of power (by the state government) without any objective material.' The petitioners in this case argued for the use of Section 69A to block specific social media websites, through which the messages apprehended to cause violence were being spread. The court, disregarding this point, maintained that the scope of operations of Section 69A and Section 144 were different and overlapped, only to cover 'public order'. The court concluded that state government, which had the rightful authority in times of emergency, deemed fit to block entire mobile Internet services, failing which, the situation would have worsened.

A Special Leave Petition (SLP) challenging the order of the Gujarat High Court in the abovementioned case of *Gaurav Sureshbhai Vyas v. State of Gujarat* was also dismissed by the Supreme Court in February 2016. While upholding the power of the state governments to restrict access to Internet, the Apex Court observed that "It becomes very necessary sometimes for law and order"[11].

Section 5(2) Indian Telegraph Act, 1855

Though Section 144 of CrPC continues to be the provision most often used to invoke blanket bans on Internet in India, Section 5(2) of Telegraph Act 1855 has also been invoked multiple times to order temporary Internet service disruptions. In fact, one of the first Internet shutdowns to be reported by mainstream media in 2012 was imposed under Section 5(2) of Telegraph Act and since then, there have been many more instances where Internet shutdowns were instituted under this provision.

Before examining Section 5(2) in further detail, let us first see how the Internet even falls within the purview of a 19th century legislation meant to govern the long-extinct domain of telegraph communications. In short, the definition of the term "telegraph" as provided under Section 3(1AA) of the Telegraph Act goes far beyond actual telegraphs, and includes *"any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means".* It is this broad and future-proof definition that brings virtually any communication system – including the Internet – within the Act's purview.

10. See https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/12/Gaurav-Vyas-v.-Guj.pdf, last accessed on April 27,2018
11. Samanwaya Rautray, *Supreme Court Upholds Internet Ban by States,* Economic Times, February 12, 2016, available at: https://tech.economictimes.indiatimes.com/news/internet/supreme-court-upholds-internet-ban-by-states/50955292, last accessed on April 27, 2018

As per Section 5(2), Central/State Governments or their authorized officers can, among other things, prevent the transmission of any telegraphic message or class of messages during a public emergency or in the interest of public safety, if it is considered necessary or expedient in the interest of (1) sovereignty and integrity of India; (2) security of the State; (3) friendly relations with foreign states; (4) public order; or (5) preventing incitement to the commission of an offence. As described earlier, the term "telegraph" can be interpreted broadly enough to cover Internet services within the ambit of the Telegraph Act and as a result, the Government's power to prevent the transmission of telegraphs also applies to the Internet. While the terms "public emergency" and "public safety", at least one of which must be present to issue an Internet shutdown order, are not defined under the Telegraph Act or any other law, they were interpreted by the Supreme Court of India in the matter of *People's Union for Civil Liberties v. Union of India*[12] to mean "the prevalence of a sudden condition or state of affairs affecting the people at large calling for immediate action", and "the state or condition of freedom from danger or risk for the people at large" respectively. Even with the Supreme Court's guidance, these terms remain open to broad interpretation by the Government, and there is no objective standard to determine if a given situation qualifies as a public emergency or threatens public safety. Also undefined are all five additional grounds described above, such as "sovereignty and integrity of India", "security of the State" and others.

In short, Section 5(2), much like Section 144 of the CrPC, is a provision of law that was clearly not designed to sanction any sort of State action with respect to the Internet and offers vast avenues for subjective interpretation of its language. This means that it is almost entirely up to the subjective interpretation of the authority issuing orders under the Section to determine if a given situation qualifies for action. Making matters worse, there were no procedural guidelines governing Internet shutdowns issued under the Telegraph Act until the Telecom Suspension Rules were issued in 2017 on how Internet shutdown orders must be issued, reviewed and enforced. In fact, there has been no indication that the ad-hoc procedure that was followed by the Government up till the Telecom Suspension Rules envisaged a review mechanism at all.

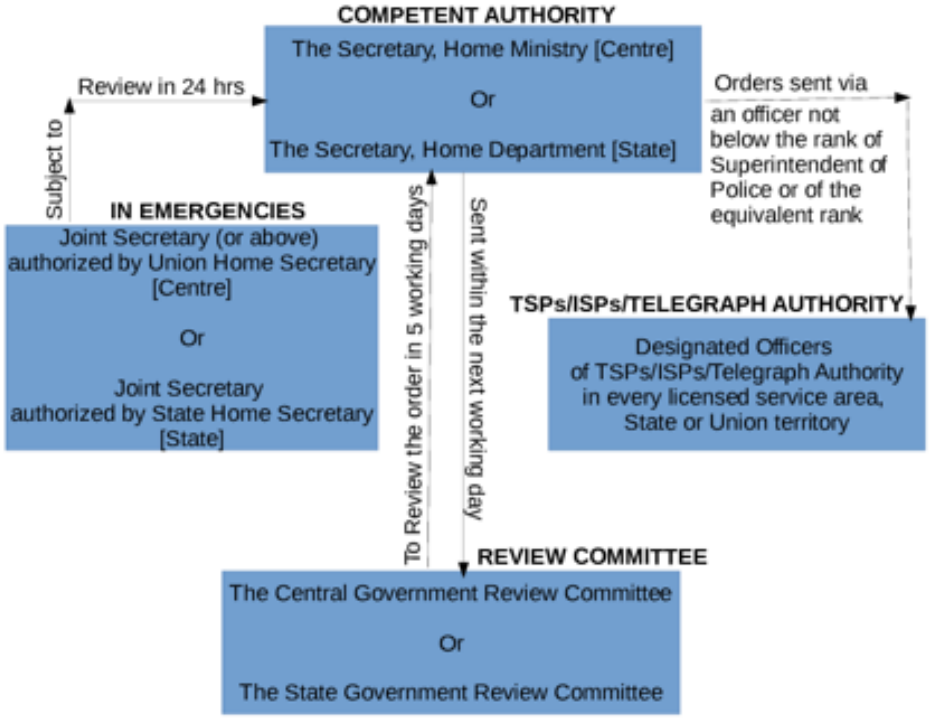
"There were no procedural guidelines governing Internet shutdowns issued under the Telegraph Act until the Telecom Suspension Rules were issued in 2017 on how Internet shutdown orders must be issued, reviewed and enforced."

Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017

The substantive law regarding suspension of Internet services was thus broadly interpreted from Section 5(2) of Telegraph Act 1855, while the procedural law regarding the same was not part of the original Act or Rules. The procedure to suspend telecom services in case of public emergency or public safety and consequently, the suspension of Internet services in India was notified under Section 7 of The Telegraph Act, 1855, on 7th August 2017. The rules are called *"Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017"*.

The 'competent authority' which may order

12. AIR 1997 SC 568



such directions are:

- In case of Government of India, the Secretary in the Ministry of Home Affairs.

- In case of a State Government, the Secretary to the State Government in-charge of the the Home Department.

According to these rules, directions to suspend telecom services shall not be issued except by an order made by a 'competent authority'. Thus, according to rule 2(1) the directions to suspend the telecom services shall be made only under these rules and according to the procedure mentioned therein. This also implies that directions for suspension of telecom services, consequently network shutdowns may not be ordered under any other provision of law, including Section 144 of CrPC 1973.

However, 'in unavoidable circumstances', such an order might be issued by an officer of the rank of Joint Secretary or above who has been duly authorised by the Union Home Secretary or State Home Secretary. But the term, 'unavoidable circumstances' has not been defined under the Telegraph Rules, Telegraph Act or any other legislation or judgments by court of law. As a result, there exists no objective standard to determine whether a given situation qualifies as an unavoidable circumstance. This raises a pertinent question: who decides whether a circumstance is unavoidable and how?

Moving ahead, the Rules also state that the order issued under 'unavoidable circumstances' will be subject to the confirmation from the competent authority

as stated above within 24 hours and will cease to exist in case of failure to obtain of such confirmation.

The rules further mandate that the order passed by the competent authority must "contain reasons for such direction" and a copy of the order shall be forwarded to a Review Committee by the next working day. The Review Committee shall comprise of:

- Where it is constituted by the Central Government- Cabinet Secretary, and Secretaries of Legal Affairs and Department of Telecommunication;

- Where it is constituted by State Government- Chief Secretary, Secretary Law or Legal Remembrancer In-Charge, Legal Affairs and Secretary to the State Government (other than the Home Secretary).

The Review Committee will have to meet within five working days of the issuance of order and record its findings on the suspension order whether it is in accordance with the provisions of sub-section (2) of section 5 of the Indian Telegraph Act.

Here ends the procedure delineated with respect to suspension of telecom services under *"Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017"*. However, there are still several areas of concern surrounding these Rules.

Firstly, the rules provide that the oversight of telecom suspension is to be carried out by a single Review Committee, which comprises entirely of the members of the executive. This severely compromises the independence and impartiality due to apparent conflict of interest when the authorization, conduct and review is carried out by a single arm of Government machinery. The public oversight principle is therefore not complied with.

Secondly, the new rules also fail to accommodate the principle of transparency. There is no provision under the rules which provide for notification of shutdowns in press or official gazettes. Considering that TSPs offering Internet services in the country do not consistently issue notifications before shutdowns are imposed, users in affected areas are often caught unaware and have little to no time to make arrangements to mitigate the impact of shutdowns.

"Considering that TSPs offering Internet services in the country do not consistently issue notifications before shutdowns are imposed, users in affected areas are often caught unawares and have little to no time to make arrangements to mitigate the impact of shutdowns."

This concludes a brief look at the provisions of law that collectively enable the Government and its agents to suspend telecom services across India.

CHAPTER 4

Internet shutdowns in India

SFLC.in has been tracking incidents of Internet shutdowns across India in an attempt to draw attention to how the number and frequency of shutdowns, which are imposed for reasons ranging from curbing unrest to preventing cheating during examinations, have been rising at an alarming rate over the years. This data is made publicly available in the form of an interactive Internet Shutdown Tracker hosted on our dedicated website www.internetshutdowns.in, which also features additional resources on the topic.

In the absence of any reliable means to gain access to Internet shutdown orders issued by various Government agents, our data is collected mostly from media reports (online and print). Over the course of the project we have expanded to include a citizen reportage mechanism i.e. a mechanism for citizens in or around affected areas to bring instances of shutdowns to attention, and provide input on how the shutdowns affected them and their communities.

Below is the comprehensive list of shutdowns that we have recorded starting January 2012. The data starts from 2012 because the earliest instance of an Internet shutdown that was reported by mainstream media came on January 26, 2012, when mobile Internet services were shut down in the Kashmir valley as part of a broader telecommunications clampdown on the occasion of Republic day. As the table reveals, there has been a staggering increase in both the number and frequency of Internet shutdowns over the years. Whereas 3 shutdowns were reported in 2012, all in the state of Jammu and Kashmir, the number rose to 70 in 2017 across 19 states. As of April 2018, 45

S.No	Year	State	Region	Reason	Kind of service restricted	Duration	Nature
1.	2018	Jammu & Kashmir	Tral and Awantipora areas of Pulwama district	Following thekilling of four Jaish-e-Muhammad (JeM) militants, one policeman and an army man in an encounter that took place between a contingent of counter-insurgent forces and militants, Mobile Internet Services were suspended in Tral and Awantipora areas of Pulwama district located in Jammu & Kashmir on Tuesday, 24th April 2018.	Mobile	No Info.	Reactive

S.No	Year	State	Region	Reason	Kind of service restricted	Duration	Nature
2.	2018	Jammu & Kashmir	Srinagar, Kulgam, Pulwama and Islamabad	Mobile Internet services were suspended in Srinagar, Kulgam, Pulwama and Islamabad districts of Jammu & Kashmir on Friday, 20th April 2018, as a precautionary measure to prevent miscreants from creating any law and order problems in the area.	Mobile	24 – 30 Hours	Preventive
3.	2018	Rajouri	Srinagar, Kulgam, Pulwama and Islamabad	Following the death of a youth, mobile internet services were suspended in Rajouri district of Jammu &Kashmir on Friday, 20th April 2018, as a precautionary measure to prevent the spread of provocative posts and pictures.	Mobile	Less than 24 Hours	Preventive
4.	2018	Jammu & Kashmir	Kathua, Samba, and Jammu	Following the reports of stone pelting in Vijaypur area, Internet services were suspended in Kathua, Samba, and Jammu districts of Jammu & Kashmir on Tuesday, 17th April 2018, as a precautionary measure to prevent the spread of rumours and hate messages.	Mobile	1-10 Hours	Preventive

5.	2018	Punjab	Kapurthala, Jalandhar, Hoshiarpur and Sahid Bhagat Singh Nagar	Mobile Internet services and SMS services were suspended in Kapurthala, Jalandhar, Hoshiarpur and Sahid Bhagat Singh Nagar districts of Punjab for three days, the suspension orders were issued on Saturday 14th April 2018, and were extended until 16th April 2018. The suspension was ordered as a precautionary measure to check rumour mongering on social media, following the Hindu-Dalit clashes over a poster of B.R. Ambedkar.	Mobile	72 Hours	Preventive
6.	2018	Uttar Pradesh	Meerut	Mobile Internet services were suspended in Meerut district of Uttar Pradesh for 24 Hours from 9 pm on Friday, 14th April 2018 till 8pm on Saturday, 15th April 2018 as a precautionary measure in the light of widespread protests by Dalits on April 2, 2018.	Mobile	Less than 24 Hours	Reactive
7.	2018	Jammu & Kashmir	Anantnag & Kulgam	Following an encounter with militants in Jammu and Kashmir's Kulgam district, which lead to killings of a civilian and an army personnel, Internet services were suspended in Anantnag & Kulgam districts of Jammu & Kashmir on Wednesday, 11th April 2018.	Mobile	48 Hours	Reactive

8.	2018	Uttar Pradesh	Saharanpur and Hapur	Following the violent clashes between supporters of the Bharat bandh and a pro-reservation group comprising OBCs and Dalits, Internet services have been suspended in Saharanpur and Hapur districts of Uttar Pradesh since midnight, 9th April 2018.	Mobile	No Info	Reactive
9.	2018	Rajasthan	Jaipur and Bharatpur	Internet services were suspended in Jaipur and Bharatpur districts of Rajasthan on Tuesday, 10th April 2018, as a precautionary measure to prevent any violence or hindrance to IPL match due to Bharat Bandh organized by Dalits.	Mobile	Less than 24 Hours	Preventive
10.	2018	Madhya Pradesh	Gwalior, Bhind, Morena and Jabalpur	Internet services were suspended in Gwalior, Bhind, Morena and Jabalpur districts of Madhya Pradesh on Monday, 9th April 2018, as a precautionary measure to prevent rumour mongering and spread of violence during Bharat Bandh on Tuesday.	Mobile	24 Hours	Preventive
11.	2018	Uttar Pradesh	Meerut, Agra, Bareilly and Saharanpur	Mobile Internet service were suspended in several districts, Meerut, Agra, Bareilly and Saharanpur of Uttar Pradesh city, on Tuesday, 3rd April 2018, as a precautionary measure, following the violent protests against Supreme Court's ruling on SC/ST Act.	Mobile	No Info.	Reactive

12.	2018	Jammu & Kashmir	Shupiyan, Pulwama, Kulgam and Anantnag and Ganderbal	Following the killing of a civilian youth in violence, mobile Internet services were suspended in four districts of South Kashmir, Shupiyan, Pulwama, Kulgam and Anantnag and Ganderbal district of Central Kashmir on Tuesday, 3rd April 2018, to pre-vent law and order problems.	Mobile	12 Hours in Central Kashmir Internet was restored after 5 days in four districts of South Kashmir, Shupiyan, Pulwama, Kulgam and Anantnag and Ganderbal	Reactive
13.	2018	Madhya Pradesh	Gwalior, Morena and Bhind	Following the killing of four people in Madhya Pradesh on Monday, 2nd April 2018, during 'Bharat Bandh' called by various Dalit organisations to protest the alleged dilution of the SC/ST (Prevention of Atrocities) Act 1989, Internet services were suspended in district Gwalior, Morena and Bhind districts of Madhya Pradesh.	Mobile	24-48 Hours	Reactive
14.	2018	Rajasthan	Jalore, Barmer, Sikar, Alwar and Ahore	Following the violent protest by Dalits, Mobile Internet services were suspended in Jalore, Barmer, Sikar, Alwar and Ahore districts of Rajasthan on Mon-day, 2nd April 2018, as a a precautionary measure to avert further violence.	Mobile	24 Hours	Reactive

15.	2018	Rajasthan	Sriganganagar and Hanumangarh	Following the violent protests by SC/ST on general category traders, Mobile Internet services were suspended in Sriganganagar and Hanumangarh districts on Monday, 2nd April 2018.	Mobile	24-48 Hours	Reactive
16.	2018	Jammu & Kashmir	South Kashmir valley	Mobile Internet services were suspended in the South Kashmir valley of Jammu & Kashmir on Sunday, 1st April 2018, as a precautionary measure following the killing of eleven militants in three separate gunfights across the state with security forces.	Mobile	24 hours	Reactive
17.	2018	Punjab	All districts	In the view of strike calls by dalit groups in Punjab, expressing concerns over the alleged "dilution" of SCs/STs (Prevention of Atrocities) Act, the Punjab government has ordered suspension of Mobile Internet services (2G/3G/4G/CDMA), all SMS services and all dongle services etc, provided on mobile networks except voice calls in the territorial jurisdiction of the state of Punjab, from 5 pm on April 1, 2018, to 11 pm on April 2.	2G/3G/4G/ CDMA), all SMS services and all dongle services etc, provided on mobile networks	24-72 hours	Preventive

18.	2018	Rajasthan	Jaitran	Following the clashes that erupted in Jaitran, a town in Rajasthan on Saturday afternoon after a few miscreants allegedly pelted stones at a procession which was being carried out on the occasion of Hanuman Jayanti, Internet Services were suspended in Jaitran town of district Jaipur in state of Rajasthan on Saturday, 31st March 2018 following as a preventive measure to avert further spreading of rumours.	Mobile	24-48 Hours	Reactive
19.	2018	Bihar	Nawada	Following the bout of violence and clashes between two communities in Nawada, internet services were suspended on Friday, 30th March, 2018 in Nawada district of Bihar.	Mobile	No Info	Reactive
20.	2018	Rajasthan	Bundi	Mobile internet services were suspended in Bundi district of Rajasthan, on 30th March 2018, as a precautionary measure to prevent any threat to peace and communal harmony in the city as a procession of Hanuman Jayanti was scheduled to be taken out in the markets on Saturday.	Mobile	No Info	Reactive

21.	2018	Bihar	Samastipur	The Internet services were suspended on Thursday, 29th March 2018, in Samastipur district of Bihar, as a preventive measure to check the spread of rumours, following the communal violence during Ram Navami procession.	Mobile	No Info.	Reactive
22.	2018	West Bengal	Asansol & Raniganj city	Internet services were suspended in Asanol & Raniganj city located in Paschim Bardhaman district in the state of West Bengal on 28th March 2018 to prevent spread of rumours following violence over a Ram Navami procession.	Mobile	7 days	Reactive
23.	2018	Bihar	Aurangabad	Internet services were suspended for 24 hours on Monday, 26th March 2018, in Aurangabad district of Bihar to contain spreading of rumours and prevent communal encounters that started over Ram Navami on Sunday.	Mobile	24 hours	Preventive
24.	2018	Jammu & Kashmir	Baramulla and Badgam	Following the killing of a Lashkar-e-Taiba militant in encounter with security forces, mobile Internet Services were suspended in Baramulla and Badgam districts of Jammu & Kashmir on Sunday, 25th March 2018.	Mobile	24 hours	Reactive

25.	2018	Odisha	Bhadrak	Internet services were suspended for 48 hours on Saturday, 24th March 2018, in Odisha's Bhadrak district as a precautionary measure to maintain communal harmony ahead of Ram Navami.	Mobile	48 Hours	Reactive
26.	2018	Jammu and Kashmir	Kulgam & Anantnag districts	Internet services were suspended on Friday, 24th March 2018, in Kulgam & Anantnag districts of Jammu & Kashmir following the killing of two Jaish-e-Mohammad militants in a brief gunfight overnight at Dooru area of south Kashmir's Anantnag district.	Mobile	No Info	Reactive
27.	2018	Rajasthan	Tonk	Section 144 was imposed and Internet services were suspended, in Tonk district of Rajasthan following the stone pelting by miscreants from a mosque at a procession marking the Hindu New Year on Sunday, 18th March 2018. The incident led to a stampede like situation, 20 people were injured and 10 were taken to hospital.	Mobile	No Info	Reactive

28.	2018	Bihar	Bhagalpur	Internet services have been suspended since Saturday, 17th March 2018 in Bhagalpur district of Bihar, to prevent communal riots.	Mobile	No Info	Reactive
29.	2018	Jammu and Kashmir	Srinagar and Anantnag	Internet services were suspended in Srinagar and Anantnag districts of Jammu & Kashmir, on Monday, 12th March 2018, as a reactive measure following the killing of three militants in Hakoora area of South Kashmir's Islamabad district.	Mobile	20 hours	Reactive
30.	2018	Jammu and Kashmir	Baramulla	Following the protests erupted in the area against the death of an elderly man who was crushed to death after police vehicle hit him, Internet services were suspended in Baramulla district of North Kashmir on March 8, 2018.	Mobile	No Info	Reactive
31.	2018	Jammu and Kashmir	Shopian and Pulwama	Mobile Internet services were suspended on 4th March 2018, in Shopian and Pulwama districts of Jammu and Kashmir as a reactive measure to prevent violence and spread of any rumour after 6 people, 2 militants and 4 civilians were killed in exchange of fire between security forces and terrorists.	Mobile	72 hours	Reactive

32.	2018	Jammu	Bandipore	Internet services were suspended on 1st March, 2018 in the Bandipora district of Jammu and Kashmir as a preventive measure following the killing of LeT millitant in a gun battle with government forces in Hajin township of North Kashmir.	Mobile	No Info	Reactive
33.	2018	Rajasthan	Tonk	Following the clashes between two communities in Tonk district of Rajasthan, mobile Internet services were suspended on 18th February 2018, for 24 hours.	Mobile	24 hours	Reactive
34.	2018	Uttar Pradesh	Firozabad	Mobile Internet services were suspended for a few hours in Firozabad district of Uttar Pradesh on 16th February 2018. The services were suspended to prevent rumour mongering in the view of alleged assault on two minority group men and a police officer by 3 BJMY members along with 20 others.	Mobile	No Info	Reactive
35.	2018	Ajmer, Alwar, Banswara, Baran, Barmer, Bharatpur, Bhilwara, Bikaner, Bundi, Churu, Chittaurgarh, Dausa, Dhaulpur, Dungarpur, Ganganagar, Hanu-	Firozabad	On 11th February, 2018 jammers were used and internet services were suspended around some exam centres across the state of Rajasthan to prevent cheating in Rajasthan Eligibility Examination for Teachers (REET).	Mobile	No Info	Preventive

35.	2018	mangarh, Jaipur, Jaisalmer, Jalor, Jhalawar, Jhunjhun, Jodhpur, Karauli, Rajasamand, Sawai Madhopur, Sikar, Sirohi, Tonk, Udaipur			Mobile	No Info	Reactive
36.	2018	Jammu and Kasmir	Kupwara, Sopore and Baramulla	Mobile Internet services were reportedly suspended in Kupwara, Sopore and Baramulla areas of Kashmir for approximately 12 hours on the night intervening 03 to 04 February 2018 to prevent rumours following reports of a Cordon and Search Operation in Kupwara. The reports were denied by police	Mobile	12 Hours	Preventive
37.	2018	Uttar Pradesh	Aligarh	Internet was shut down from 27 January 2018 to 10 pm on 28 January 2018 in Kasganj district of Uttar Pradesh following violent clashes that have ensued since the death of a 16 year old boy in stone pelting and firing of gun(s) on Republic Day - 26 January 2018. The area was already under curfew for a day before the shutdown was imposed.	Mobile	24 hours	Reactive

38.	2018	Jammu and Kashmir	Anantnag, Bandipore, Badgam, Baramula, Ganderbal, Kupwara, Pulwama & Srinagar	Mobile Internet was shut down on January 25 at 7:30 PM across the entire Kashmir Valley in anticipation of militant activity on Republic Day - January 26.	Mobile	24 hours	Preventive
39.	2018	Jammu and Kashmir	Shupiyan, Pulwama, Anantnag & Kulgam	Pulwama, Shupiyan, Anantnag and Kulgam faced an Internet shutdown starting from 24 January 2018, while the rest of Kashmir's Internet speeds were reduced to 128 kbps following the death of two militants and a civilian.	Mobile	No info	Preventive
40.	2018	Jammu and Kashmir	Anantnag & Kulgam	Mobile Internet service were suspended in the twin districts of Anantnag and Kulgam of Kashmir on 9th January, 2018 following clashes in Larnoo area after protests by youth to disrupt the anti-militant operation wherein one militant was killed by the government forces. The services were reportedly restored in the area in the morning of 11th January, 2018.	Mobile Internet services	42 hours	Reactive
41.	2018	Jammu and Kashmir	Badgam	Mobile Internet service in central Kashmir's Badgam district were suspended yet again on 8th January, 2018 to prevent rumour mon-gering as a gunfight raged between militants and government forces in Patrigam village of Chadoora.	Mobile Internet services	No info	Preventive

42.	2018	Maharashtra	Kolhapur	Following protests by Dalit groups during the day-long bandh, called to protest against the violence post the celebrations of Bhima Koregaon battle, Internet services were suspended in Kolhapur district of Maharashtra on 4th January, 2018 for a period of 24 hours due to escalating tension in the district.	No info.	24 hours	Reactive
43.	2018	Maharashtra	Aurangabad	In the wake of Maharashtra bandh called by Dalit organisations protesting the clashes at the bicentenary celebrations of the battle of Bhima-Koregaon on 1st January, Internet services were suspended on 3rd January, 2018 in Aurangabad district of Maharashtra.	Mobile Internet	No info	Reactive
44.	2017	Rajasthan	Bundi	Amid the call given by some Hindu organizations to perform puja on 1st January at Maandhata Balaji Temple in Bundi city, Kota divisional commissioner on Saturday issued orders to temporarily suspend internet services including 2G, 3G, 4G data, bulk SMS, Whatsapp, Facebook, Twitter and other social sites in Bundi district for 48 hours, from 6am on 31st December to 6am on 2nd January, 2018.	Mobile Internet	24-72 hours	Preventive

45.	2017	Jammu and Kashmir	Pulwama	Mobile Internet services were suspended in Pulwama district of Jammu and Kashmir on 31st December, 2017 after a group of militants entered into commando training centre (CTC) of CRPF at Lethpora area of Pulwama triggering fierce gunfights.	Mobile Internet	No info.	Preventive
46.	2017	Jammu and Kashmir	Pulwama	Mobile Internet was suspended in the Pulwama district of Kashmir on 26th December, 2017 following the killing of top Jaish-e-Muhammad commander Noor Muhammad.	Mobile Internet	No info.	Preventive
47.	2017	Jammu and Kashmir	Pulwama and Shopian	Mobile Internet services were suspended for three days in the twin districts of Pulwama and Shopian in south Kashmir on 18th December, 2017 in the wake of a gunfight between militants and government forces in Batmurran village of Shopian district.	Mobile Internet	72 hours	Preventive
48.	2017	Jammu and Kashmir	Kupwara	Mobile internet services were suspended in Kupwara district of Jammu and Kashmir on 17th December, 2017 as a precautionary measure after protests erupted over the death of a taxi driver who was killed in Army firing.	Mobile Internet	72 hours	Reactive

49.	2017	Telangana	Adilabad	Internet services were suspended in Adilabad district of Telangana on 16th December, 2017 as a precautionary measure to curb the spread of rumours on social media in the wake of clashes between Adivasis and Lambadas	No info	No info.	Preventive
50.	2017	Udaipur and Rajsamand	Adilabad	Mobile Internet services were suspended in Udaipur and Rajsamand district of Rajasthan in the evening of 13th December, 2017 as a precautionary measure for a period of 24 hours after some Hindu organizations announced a rally in support of Shambhu Raigar, who brutally murdered a Muslim man and filmed the act over love jihad.	Mobile Internet	24 hours	Preventive
51.	2017	Jammu and Kashmir	Sopore, Baramulla, Handwara, Kupwara	Mobile Internet services were suspended on 11th December, 2017 in Sopore, Baramulla, Handwara and Kupwara districts of Jammu and Kashmir as a precautionary measure following the kiling of three militants in Handwara's Yunso village	Mobile Internet	No info	Preventive

52.	2017	Rajasthan	Bhilwara, Chittorgarh, Nimbahera	Internet services were suspended in Bhilwara, Chittorgarh and Nimbahera of Rajasthan on 3rd December, 2017 to prevent rumours from spreading on social media after clashes between two communities broke out when muslim community was taking out barawafat procession on the occasion of Eid-e-Milad.	No info	No info.	Reactive
53.	2017	Haryana	Jind, Hansi, Bhiwani, Hisar, Fatehabad, Karnal, Panipat, Kaithal, Rohtak, Sonipat, Jhajjar, Bhiwani, Charkhi Dadri	Mobile Internet services were suspended on 11th December, 2017 in Sopore, Baramulla, Handwara and Kupwara districts of Jammu and Kashmir as a precautionary measure following the kiling of three militants in Handwara's Yunso village	Mobile Internet	25 to 72 hours	Preventive
54.	2017	Jammu and Kashmir	Pulwama	Internet services were suspended in Pulwama district of Kashmir on 2nd November, 2017 following a gunfight in which two army soldiers and a militant were killed in Pulwama.	Mobile Internet services	No info.	Preventive

55.	2017	Bihar	Arwal, Bhojpur, Jamui, Katihar, Sitamarhi, West Champaran	Internet services were suspended in several districts of Bihar including Arwal, Jamui, Bhojpur, Katihar, Sitamarhi and West Champaran on 1st October, 2017 to check spreading of rumours following instances of communal violence in the districts. The services were reported to have been restored in Bhojpur on 4th morning, in Jamui on 4th October midnight while in other districts on 5th October.	No info	More than 72hrs	Reactive
56.	2017	Bihar	Nawada	Internet services were suspended in Nawada district of Bihar on 28th September, 2017 till 5th November to prevent spread of any inflammatory message on social media after communal tension gripped some areas in the district when an idol of Goddess Durga was damaged in stone pelting by a group of anti-social elements.	No info	More than 72 hours	Reactive
57.	2017	Jammu and Kashmir	Baramulla	Kashmir saw yet another shutdown as mobile Internet services were suspended in Baramulla district, including Sopore town, on 26th September, 2017 to prevent rumours after the killing of top militant commander Abdul Qayoom Najar.	Mobile Internet services	No Info	Preventive

58.	2017	Tripura	Agartala	Internet services were suspended as a preventive measure in Agartala city of Tripura on 21st September, 2017 following the killing of a journalist, who was covering a clash between two political parties in Mandwai of West Tripura. The services were reportedly restored on 25th September, 2017.	No info	More than 72 hrs	Preventive
59.	2017	Jammu and Kashmir	Kulgam, Anantnag	Mobile Internet services were suspended in Kulgam and Anantnag districts of Jammu and Kashmir on 11th September, 2017 to prevent spreading of rumours after two militants were killed in a gunfight with government forces.	Mobile	Info not available	Preventive
60.	2017	Rajasthan	Sikar	Mobile and broadband Internet services were suspended in Sikar district of Rajasthan on 11th September, 2017 to prevent law and order circumstances after the situation became intense with farmers setting off on a march to seize the collectorate following the ongoing farmers' protest in the State.	Both	Info not available	Preventive
61.	2017	Jammu and Kashmir	Baramula	Internet services were suspended on 9th September, 2017 in the Sopore town of Baramula district in Jammu and Kashmir as a preventive measure after a gunfight between militants and security forces broke out in the town.	Info not available	Info not available	Preventive

62.	2017	Rajasthan	Jaipur	Mobile Internet services were imposed in several parts of Jaipur city in Rajasthan on 9th September, 2017 as a reactive measure after one person was killed and 11 others were injured in a clash between locals and police personnels in the city.	Mobile Internet	Info not available	Reactive
63.	2017	Haryana	Sirsa	Mobile Internet sevices were suspended in Sirsa district of Haryana on 8th September, 2017 till 10th September to prevent rumour mongering and disturbance of public order in view of the 'sanitisation' process being carried out at the Dera Sacha Sauda headquarters.	Mobile Internet	25 to 72 hours	Preventive
64.	2017	Bihar	Madhepura, Supaul, Saharsa, Purnia, Araria, Kishanganj, Katihar	Internet services were suspended in seven districts of Bihar on 5th September, 2017 as a precautionary measure to prevent spread of rumours following communal tensions after dozens of slaughthered cattle carcasses were found floating in a canal in Bihar's Madhepura district.	Info not available	25 to 72 hours	Preventive

65.	2017	Jammu and Kashmir	Kupwara	Mobile Internet services were suspended yet again in Kupwara district of Jammu and Kashmir on 4th September, 2017 as a precautionary measure after two Hizbul Mujahideen militants were killed in a gunfight in Sopore district of Kashmir.	Mobile Internet	Info not available	Preventive
66.	2017	Jammu and Kashmir	Shopian, Kulgam	Mobile Internet services were suspended in Shopian and Kulgam districts in Jammu and Kashmir on 2nd September, 2017 as a reactive measure after clashes broke out following the killing of a LeT terrorist in an encounter with the security forces.	Mobile Internet	Info not available	Reactive
67.	2017	Jammu and Kashmir	Pulwama	After a 'Fidayeen' attack by the militants on District Police Lines, mobile Internet services were suspended in Pulwama district of Kashmir on 26th August, 2017 as a precautionary measure to prevent law and order situation	Mobile Internet	Info not available	Preventive
68.	2017	Ganganagar, Hanumangarh	Pulwama	Following the conviction of Dera Sacha Sauda chief Gurmeet Ram Rahim Singh in a rape case, mobile Internet services were suspended in the districts of Sriganganagar and Hanumangarh on 25th August, 2017 for 48 hours in response to the violent backlash from the Dera followers.	Mobile Internet	25 to 72 hours	Reactive

69.	2017	Chandigarh	Chandigarh	Ahead of the verdict in the rape case against Dera Sacha Sauda chief Gurmeet Ram Rahim Singh, mobile Internet services were suspended in Chandigarh on 24th August, 2017 for 72 hours as a precautionary measure anticipating violent backlash from the Dera followers.	Mobile Internet	25 to 72 hours	Preventive
70.	2017	Haryana	All the districts of Haryana	Ahead of the verdict in the rape case against Dera Sacha Sauda chief Gurmeet Ram Rahim Singh, mobile Internet services were suspended in Haryana on 24th August, 2017 for 72 hours as a precautionary measure anticipating violent backlash from the Dera followers. The ban was further extended till 29th August, 2017. While the internet was restored in other parts, it continued to remain suspended in seven 'sensitive' districts of Haryana till 30th August, 2017	Mobile Internet	More than 72 hours	Preventive
71.	2017	Punjab	All the districts of Punjab	Ahead of the verdict in the rape case against Dera Sacha Sauda chief Gurmeet Ram Rahim Singh, mobile Internet services were suspended in Punjab on 24th August, 2017 for 72 hours as a precautionary measure anticipating violent backlash from the Dera followers. The ban was further extended till 29th August, 2017	Mobile Internet	More than 72 hours	Preventive

72.	2017	Jammu and Kashmir	Pulwama	Mobile Internet services were suspended yet again in Pulwama district of Kashmir on 16th August, 2017 to prevent rumour mongering after a Lashkar commander was killed in a gunfight with the security forces.	Mobile Internet	Ongoing	Preventive
73.	2017	Jammu and Kashmir	Kashmir Valley	Mobile and broadband Internet services were suspended in the Kashmir valley in the morning of 15th August, 2017 as a precautionary measure on Independence Day. Services were reportedly restored later in the day.	Both	Less than 24 hours.	Preventive
74.	2017	Jammu and Kashmir	Shopian, Kulgam	Internet services were suspended in Shopian and Kulgam district of Kashmir on 13th August, 2017 to prevent the spreading of information after three Hizbul Mujahideen militants including the operations commander, and two army men were killed in an encounter.	No Info.	Ongoing	Preventive
75.	2017	Jammu and Kashmir	Pulwama	Internet services were suspended in Pulwama district of Kashmir on 9th August, 2017 as a precautionary measure after three militants were killed in a gunfight with the Government forces in the Tral township. However, the services on state-owned Bharat Sanchar Nigam Limited remained functional.	No Info.	Ongoing	Preventive

76.	2017	Jammu and Kashmir	Baramulla	Mobile Internet services were suspended in Baramulla district of Kashmir as a precautionary measure on 5th August, 2017 after three LeT militants were killed in an encounter with the security forces in the Sopore town of the district.	Mobile Internet	Ongoing	Preventive
77.	2017	Jammu and Kashmir	Kashmir Valley	Mobile Internet services were suspended yet again across Kashmir on 1st August, 2017 as a precautionary measure fearing clashes after the killing of Lashkar-e-Toiba commander Abu Dujana and his aide in an encounter with the security forces. The services were restored on 2nd August, 2017 after remaining suspended for over 24 hours.	Mobile Internet	24 hours or more	Preventive
78.	2017	Jammu and Kashmir	Pulwama	Mobile Internet services were suspended in Pulwama district of Kashmir on 30th July, 2017 as a preventive measure to prevent spreading of rumours following the killing of two militants in a shootout in Tahab village.	Mobile Internet	No info.	Preventive

79.	2017	Jammu and Kashmir	Budgam	Mobile Internet services were suspended on 21st July, 2017 in Budgam district of Kashmir as a precautionary measure after a young tailor was killed in army firing in Beerwah town of the district. The services were reported to have been restored on 25th July, 2017, four days after they were suspended.	Mobile Internet	73 hours or more	Preventive
80.	2017	Tripura	Agartala, all districts	Internet services were suspended in Tripura on the morning of 20th July, 2017 to prevent Indigenous Peoples Front of Tripura (IPFT) from spreading false propoganda following the eleven day blockade demanding a separate tribal State 'Tipraland'. The services were restored on 20th July, 2017- 14 hours after they were shut.	No info	Less then 24 hours.	Preventive
81.	2017	Jammu and Kashmir	Kashmir Valley	While mobile Internet services were already shut, broadband services too were snapped in Kashmir Valley on 18th July, 2017 as a precautionary measure after the killing of three terrorist in an encounter with the security forces.	Broadband	No info.	Preventive

82.	2017	Jammu and Kashmir	Kashmir Valley	Mobile Internet services were shut down yet again as a precautionary measure in Anantnag district on 16th July, 2017 following the killing of militants in gun-battle with forces on 15th July.	Mobile Internet	No info	Preventive
83.	2017	Gujarat	Morbi, Surendranagar	Internet services were suspended in Morbi and Surendranagar districts of Gujarat on 14th July, 2017 to prevent rumour mongering on social media following violent clashes between members of Bharwad and Rajput communities. The services were restored on 18th July, 2017.	Info not available	73 hours or more	Preventive
84.	2017	Rajasthan	Nagaur, Bikaner, Churu, Sikar	Internet services were suspended in the evening of 11th July, 2017 in the districts of Nagaur, Bikaner, Churu and Sikar to prevent spread of rumours after the violence in Sanvrad with Rajput community demanding Central Bureau of Investigation (CBI) enquiry in the encounter of gangster Anand Pal Singh. The services reportedly resumed on 14th July, 2017.	No info	24-72 hours.	Preventive

85.	2017	Jammu and Kashmir	Jammu	Both Internet and broadband services were suspended in Jammu late at night on 10th July, 2017 as a precautionary measure following the killing of Amarnath pilgrims in a militant attack in the Kashmir Valley. The services were reportedly restored on 12th July, 2017, 36 hours after they were suspended.	Both	25-72 hours	Preventive
86.	2017	Jammu and Kashmir	Kashmir Valley	Just a day after the Internet services were restored, both mobile and broadband Internet services were again suspended in the Kashmir Valley in the night of 10th July, 2017 at 10 pm as a precautionary measure after the appeal of separatists to people to launch a "Kashmir awareness" campaign on social media on 11th July. However, the services were restored in the midnight after remaining suspended for around two hours.	Both	24 hours or less	Preventive
87.	2017	Jammu and Kashmir	Kashmir Valley	Both mobile and broadband Internet services were suspended in the Kashmir Valley on 6th July, 2017 as a precautionary measure in view of law and order situations on the first death anniversary of Hizbul Mujahideen 'commander' Burhan Wani. While the 2G mobile Internet services were restored on the night of 8th July, 2017, broadband services were restored in the morning of 9th July, 2017.	Both	25 to 72 hours	Preventive

88.	2017	West Bengal	North 24 Parganas	Baduria and Basirhat areas of North 24 Parganas district in West Bengal saw suspension of Internet services on 5thJuly, 2017 after violent communal clashes broke out over an objectionable Facebook post by a 17 year old boy. The services were restored on July 10th, 2017 in Basirhat.	Info not available	73 hours or more	Reactive
89.	2017	Jammu and Kashmir	Anantnag	Mobile Internet services were shutdown on 1st July, 2017 to prevent rumour mongering on social media websites after violent clashes between militants and government forces in Brenthi Dialgam village.	Mobile Internet	No info	Reactive
90.	2017	Rajasthan	Churu, Nagaur	Mobile Internet was suspended on 30th June, 2017 to prevent rumour mongering after the protests by the Rajput community over the encounter killing of gangster intensified. The services were reportedly restored on July 5, 2017.	Mobile Internet	73 hours or more	Preventive

91.	2017	West Bengal	Darjeeling	Days after mobile Internet services were shutdown in Darjeeling, broadband services were also suspended in the area for a period of 7 days on 20th June, 2017 in the interest of public safety, following the indefinite strike by Gorkha Janmukti Morcha (GJM) for a separate Gorkhaland.	Broadband	Ongoing	Preventive
92.	2017	West Bengal	Darjeeling	Mobile Internet services were blocked in Darjeeling on 18th June, 2017 following deaths of party supporters in violent clashes between the Gorkha Janmukti Morcha and security forces after the former called for a complete strike in its agitation for a separate Gorkhaland.	Mobile Internet	Ongoing	Reactive
93.	2017	Jammu and Kashmir	Kashmir Valley	Mobile Internet was shutdown again in Kashmir Valley on 16th June, 2017 as a precautionary measure after firing by the security forces'caused the death of a youth leading to escalated tensions in the region. The services resumed on June 19th, 2017.	Mobile Internet	73 hours or more	Preventive

94.	2017	Uttar Pradesh	Saharanpur	Internet services were suspended in Saharanpur district yet again on 8th June, 2017 following the arrest of the main accused in Saharanpur violence, for a period of two days, to prevent any unrest. The services were reportedly restored in the afternoon of 12th June, 2017.	Info not available	73 hours or more	Preventive
95.	2017	Jammu and Kashmir	Kashmir Valley	Kashmir Valley witnessed another suspension of mobile Internet services on 7th June, 2017 after the death of a civilian in firing by security forces.	Mobile Internet	No info	Preventive
96.	2017	Madhya Pradesh	Mandsaur, Ratlam, Ujjain, Neemuch, Indore, Dewas	Internet services were suspended in the districts of Mandsaur, Ratlam, Ujjain, Neemuch, Indore, Dewas on 6th June, 2017 following the farmers' protest in Madhya Pradesh demanding higher rates for their produce. The services were restored on 11th June, 2017.	Info not available	73 hours or more	Preventive
97.	2017	Maharashtra	Nashik	Mobile Internet services were suspended in Nashik for a few hours on 5th June, 2017 as the State-wide strike called by farmers turned violent in the former area.	Mobile Internet	Less than 24 hours	Reactive

98.	2017	Jammu and Kashmir	Kashmir Valley	Mobile Internet services were suspended yet again in the Kashmir Valley region as a preventive measure on 27th May, 2017 in order to check rumour mongering following the encounter of a Hizbul terrorist. The services were reportedly restored on 2nd June, 2017.	Mobile Internet	More than 72 hours	Preventive
99.	2017	Uttar Pradesh	Saharanpur	Mobile Internet services were suspended in Saharanpur on 24th April, 2017 to contain rumour mongering on social media amid violent caste based clashes between Dalit and Rajput community. The services were restored after 10 days on June 3, 2017	Mobile Internet	73 hours or more	Reactive
100.	2017	Odisha	Kendrapara	Internet services were reportedly suspended for 48 hours in Kendrapara on 19th April, 2017 to prevent rumor mongering over a social media post with objectionable content. The services were reported to be restored on 21st April, 2017.	Info not available	25 to 72 hours	Preventive
101.	2017	Rajasthan	Udaipur and Fatehnagar	As a precautionary measure, mobile Internet services were suspended in Udaipur and Fatehnagar areas on late 18h April, 2017 to curb the escalation of tensions over a social media post saying, "Pakistan zindabad hai, aur zindabad rahega.". The service was reported to be restored on 19th April, 2017.	Mobile Internet	24 hours or less	Preventive

102.	2017	Jammu and Kashmir	Kashmir Valley	Mobile Internet services were ordered to be suspended yet again on 17th April, 2017 as students across the Valley held protests against the recent clashes between students and police in Pulwama district. Moreover, social media websites were ordered to be restricted even on fixed line networks to restrict the spread of rumors and messages. The mobile Internet services were reportedly restored on 29th April, 2017 following the direction of the State Government to block access to 22 social media sites and applications on all platforms.	Mobile Internet	73 hours and more	Reactive
103.	2017	Jammu and Kashmir	Kashmir Valley	On 13th April, 2017, broadband services were suspended yet again in light of re-polling in 38 stations of Budgam district. Both, broadband services, as well as mobile Internet that was suspended since 9th April, 2017 was restored in the evening of 13th April, 2017.	Both	Less than 24 hours	Preventive
104.	2017	Odisha	Bhadrak	As a preventive measure in the area that recently witnessed communal violence over derogatory remarks about Hindu deities, Internet services were reportedly suspended for 48 hours under Section 5 of the Telegraph Act on 9th April, 2017. These services were reportedly restored on 11th April, 2017.	Information not	25 to 72 hours	Preventive

105.	2017	Jammu and Kashmir	Kashmir Valley	Both, mobile and broadband services were suspended from midnight in three districts of Srinagar, Budgam, and Gandarbal on 8th April, 2017 as a precautionary measure to curb spread of rumors ahead of the Srinagar bypoll. However, the restriction on Internet services was extended to the entire Kashmir valley on 9th April, 2017. While broadband services were restored on 11th April, 2017, mobile Internet services remained suspended till 13th April, 2017.	Both	Broadband: 25 to 72 hours Mobile: 73 hours or more	Preventive
106.	2017	Rajasthan	Sikar	Mobile Internet services were suspended in the Sikar district of Rajasthan on 31st March, 2017 after clashes amongst youngsters during a religious procession resulted in stone-pelting, injuring one policeman. Mobile Internet services were restored in the evening on 6th April, 2017.	Mobile Internet	73 hours or more	Reactive
107.	2017	Haryana	Rohtak, Sonipat, Jhajjar, Bhiwani, Panipat, Hisar, Kaithal, Charkhi Dadri, Fatehabad, Jind and Sirsa	Mobile Internet services were suspended in 'sensitive' districts including Rohtak, Sonipat, Jhajjar, Bhiwani, Panipat, Hisar, Kaithal, Charkhi Dadri, Fatehabad, Jind and Sirsa on 18th March, 2017 as a precautionary measure in the wake of Jat protests outside the Parliament. The services were restored on 19th March, 2017.	Mobile Internet	24 hours or less	Preventive

108.	2017	Haryana	Rohtak and Sonepat	Internet services were suspended in the districts of Rohtak and Sonepat for 24 hours – from 5 pm on 25th February to 26th February, 2017 while the Jats observed 'Black Day' in Haryana on February 26, 2017.	No conclusive information available	24 hours or less	Preventive
109.	2017	Haryana	Jhajjar, Panipat, Sonipat, Hisar, Rohtak, Jind and Bhiwani	Mobile Internet services were suspended indefinitely on 17th February, 2017 in the districts of Jhajjar, Panipat, Sonipat, Hisar, Rohtak, Jind, and Bhiwani following violent protests during the ongoing Jat agitations, and were reportedly restored on 19th February, 2017.	Mobile Internet	25 to 72 hours	Reactive
110.	2017	Haryana	Rohtak, Bhiwani, Hisar, Sonipat, Panipat	Mobile Internet was suspended in districts of Rohtak, Bhiwani, Hisar, Sonipat, and Panipat starting 31st January, 2017 due to the ongoing Jat agitations in various parts of the state.	Mobile Internet	No Info On	Preventive
111.	2017	Nagaland	Entire state	Mobile Internet services were disrupted in the entire state starting 30th January, 2017 as clashes ensued between the locals and police over the State government's decision to apply reservation in civic body elections. The services were restored on 20th February, 2017.	Mobile Internet	73 hours or more	Reactive

112.	2017	Haryana	Jhajjar	Owing to the agitations being held by the Jat community, mobile Internet services were suspended in Jhajjar starting 29th January, 2017.	Mobile Internet	No Info	Preventive
113.	2016	Nagaland	Wokha and Phek	Mobile Internet services were suspended in Wokha and Phek districts starting 19th January, 2017 due to violence in the area on the issue of reservation in local body elections. The suspension later spread to the entire state of Nagaland on 30th January, 2017, and Internet services resumed on 20th February, 2017.	Mobile Internet	73 hours or more	Reactive
114.	2016	Rajasthan	Bhilwara	Internet services were suspended in the district of Bhilwara to maintain law and order for reportedly 72 hours starting 27th December, 2016 as the Nagrik Suraksha Manch (a citizens' group) called for a city wide Bandh to protest lack of action taken against the accused in the ongoing communal riots.	No conclusive information	25 to 72 hours	Preventive
115.	2016	Rajasthan	Bhilwara	Mobile internet services were disrupted in the district of Bhilwara on 19th December, 2016 due to the ongoing communal tensions.	Mobile internet	No conclusive info	Reactive

116.	2016	Manipur	East and West Imphal	Orders were issued by the District Magistrate to disconnect mobile Internet services in East and West Imphal from 18th December, 2016 due to law and order turmoil over economic blockade by the United Naga Council (UNC). Mobile Internet services were reportedly restored on 30th December, 2016 after a 12 day disruption.	Mobile Internet	More than 72 hours	Reactive
117.	2016	Rajasthan	Bhilwara	Internet services were suspended under Section 144 on 13th December 2016 till 5 pm in the district of Bhilwara due to the onslaught of communal tensions coinciding with the preparations of a Muslim religious function, Barafwat.	No conclusive information	24 hours or less	Reactive
118.	2016	Jammu and Kashmir	Anantnag	Mobile phone services were reportedly suspended in parts of Kashmir, including Anantnag on 8th December, 2016 as a gun-fight ensued between militants and the security forces.	No information available	24 hours or less	Reactive
119.	2016	Bihar	Bhojpur, East Champaran, Gopalganj	Both, mobile and broadband internet services were disconnected from 15th October to prevent misuse of social media platforms due to violent communal clashes in the area. They were restored in Bhojpur on 18th October, 2016, whereas East Champaran was connected back to internet on 20th October, 2016.	Both	More than 72 hours	Reactive

120.	2016	Maharashtra	Nashik	Mobile Internet services and bulk SMS were blocked for two days (48 hours) on 10th October, 2016 in Nashik district as protests emerged over the alleged rape attempt of a 5 year old girl by a teenage boy.	Mobile Internet	25-72 hours	Reactive
121.	2016	Uttar Pradesh	Bijnor district	Internet services were suspended in the Bijnor district on 18th September, 2016 for reportedly 48 hours after communal clashes ensued in the region due to the alleged harassment of a school girl.	N/A	25-72 hours	Reactive
122.	2016	Rajasthan	Bhilwara	Internet services were blocked for 24 hours in Bhilwara on 16th September, 2016 after the stabbing of a 21 year old as he was returning home from Ganpati Puja.	N/A	24 hours or less	Reactive
123.	2016	Jammu & Kashmir	Kashmir	Ahead of Eid celebrations, fixed-line Internet services were suspended in Kashmir on 12th September, 2016 as a precautionary measure in light of the ongoing violence in the region. These services were reportedly resumed on 17th September, 2016. However, mobile Internet services remain suspended since 9th July, 2016.	Both	More than 72 hours	Preventive
124.	2016	Jammu & Kashmir	Kashmir valley	After the disconnect from mobile internet services since 9th July, 2016, broadband internet services were also suspended in the Kashmir valley on 13th August, 2016 for 5 days as a precautionary measure to prevent rumor mongering due to unrest between the protestors and the security forces.	Both	More than 72 hours	Preventive

125.	2016	Arunachal Pradesh	Itanagar	Mobile internet services were disrupted for two days in Itanagar, Arunachal Pradesh on 10th August, 2016 following the death of former Chief Minister of Arunachal Pradesh, Kalikho Pul.	Mobile Internet	25-72 hours	Reactive
126.	2016	Bihar	Saran district	Due to communal clashes in the Saran district after a video of the desecration of hindu deities went viral on social media, all internet services were shut down in the district under Section 144 of CrPC on 6th August, 2016 till 8th August, 2016 to prevent spread of rumors.	No conclusive information	25-72 hours	Reactive
127.	2016	Jammu & Kashmir	Jammu region	Due to bandhs being declared in the Chenab valley to show solidarity with protests being undertaken by Kashmiris, mobile internet services were suspended in Jammu region on 5th August, 2016. The services were reportedly restored on the same day.	Mobile internet	24 hours or less	Reactive
128.	2016	Jammu & Kashmir	Pulwama district and the towns of Ananatnag, Shopian, Pulgam and Sopore, and some parts of Srinagar	Following the killing of Burhan Wani, Kashmir valley and the Jammu region experienced a suspension of mobile internet services to check the spread of rumors by anti-social elements on 9th July, 2016. However, mobile internet services were restored in Jammu region on 26th July, 2016; after being suspended for 17 days. Reportedly, mobile internet services were restored in Kashmir valley on 19th November for post paid connections and on 27th January, 2017 for pre-paid connections.	Mobile internet	More than 72 hours	Reactive

129.	2016	Rajasthan	Barmer and Jaisalmer	After the death of a person in police firing, mobile internet services were shut down in Barmer and Jaisalmer for 48 hours on 30th June, 2016 as calls for a Bandh was announced by the community members of the person who was killed.	Mobile Internet	25-72 hours	Reactive
130.	2016	Jammu & Kashmir	Poonch district	Over a controversial issue, mobile internet services were suspended in the Poonch district on 22nd June, 2016 on operational and security grounds and to prevent law and order situations and were restored the same day.	Mobile Internet	24 hours or less	Preventive
131.	2016	Jammu & Kashmir	Jammu	Mobile internet services were suspended in Jammu region on 22nd June, 2016 ahead of a wrestling match, the venue for which is disputed between two communities, and experienced violence in 2014 as well. There is no exact information available as to when the services were restored.	Mobile internet services	No info available	Preventive
132.	2016	Jammu & Kashmir	Entire state	Mobile internet services were suspended in the entire state after a youth resorted to vandalization and desecration of a temple in Jammu, that led to a spur of violence in the region on 15th June, 2016. The services were reportedly restored on 18th June, 2016.	Mobile internet services	More than 72 hours	Reactive
133.	2016	Haryana	Rohtak	Mobile internet services and bulk SMS were blocked in Rohtak on 5th June, 2016 , along with the prolonged shut down in Sonipat as well, to curb the use of social media from instigating violence in the Jat agitation. There is no information available regarding the restoration of internet services.	Mobile internet services	No info	Preventive

134.	2016	Haryana	Sonipat	Mobile internet services were blocked in Sonipat, Haryana on 4th June, 2016 until further notice to prevent spread of misinformation prior to the agitation organized by the Jat community on 5th June, 2016. There is no information available regarding the restoration of internet services.	Mobile Internet	25-72 hours	Reactive
135.	2016	Uttar Pradesh	Azamgarh	In Azamgarh, the local administration resorted to suspension of mobile & broadband services from 16th to 18th May, 2016 as a precautionary measure to check the outbreak of riots due to communal tension in the area.	Both	25 to 72 hours	Preventive
136.	2016	Gujarat	Ahmedabad, Mehsana, Surat and Rajkot,	Pursuant to the Patel reservation agitation, mobile internet sevices were suspended in various parts of Gujarat on 17th April, 2016 and restored on 19th April, 2016.	Mobile internet	25 to 72 hours	Reactive
137.	2016	Jharkhand	Bokaro	Subsequent to the communal clashes in the city of Bokaro during celebration of Ram Navami, internet services were cut off from 16th April, 2016 to 18th April, 2016 to prevent spreading of communal fear and hatred through social media.	No info available	25 to 72 hours	Reactive
138.	2016	Jammu & Kashmir	North Kashmir, Srinagar and south Kashmir's Pulwama district	To check rumor mongering about an incident that led to death of 4 people in a firing by security forces, mobile internet services were suspended in the area on 14th April, 2016 and restored on 18th April, 2016	Mobile internet services	More than 72 hours	Reactive

139.	2016	Haryana	Rohtak, Jhajjar	Mobile internet services were suspended in various districts in Haryana as a prohibitory measure in light of the possible re-agitation of the Jat community for classification as Other Backward Classes (OBC) on 18th March, 2016 and restored on the same day.	Mobile Internet	24 hours or less	Preventive
140.	2016	Gujarat	Mehasana	Mobile Internet services were suspended in the district of Mehasana on 28th February, 2016 for 12 hours from 8 am to 8 pm as the Patidar Anamat Andolan Samiti (PAAS) decided to continue with their women's conference despite being officially refused permission by the district Government.	Mobile Internet	24 hours or less	Preventive
141.	2016	Gujarat	Entire state of Gujarat	Mobile Internet services were suspended for 4 hours in the entire state to prevent cheating on the Revenue Accountants Recruitment Exam on 28th February, 2016	Mobile Internet	24 hours or less	Preventive
142.	2016	Rajasthan	Bharatpur	Due to the agitations of the Jat community for reservations as OBC, internet services were shut down on 22nd February, 2016 and restored on the evening of 23rd February,	No info available	24 hours or less	Reactive
143.	2016	Haryana	Jhajjar, Panipat, Sonipat, Hisar, Rohtak, Jind and Bhiwani	Subsequent to the Jat reservation protest in Haryana, mobile Internet, and SMS services were blocked in many areas beginning 19th February, 2016.	Mobile internet	No info available	Reactive
144.	2016	Jammu & Kashmir	Kashmir	On the occasion of Republic Day, mobile internet services were snapped for a few hours as a precautionary measure on 26th January, 2016	Mobile internet	24 hours or less	Preventive

145.	2015	Jammu & Kashmir	Kashmir	On the visit of Prime Minister, Narendra Modi, the mobile internet services were temporarily blocked in the Kashmir region as a precautionary measure for his high profile address at a public rally on 7th November, 2015.	Mobile Internet	24 hours or less	Preventive
146.	2015	Rajasthan	Bhilwara	In an incident of communal tension over the alleged killing of a muslim youth, internet services were suspended in both these areas for 24 hours on 24th October, 2015.	Info not available	24 hours or less	Reactive
147.	2015	Gujarat	Rajkot	On 17th October, 2015, mobile internet services were suspended for 2 days in the area due to threats made by Hardik Patel to hold a protest in the stadium where a one day international cricket match was scheduled between the teams of India & South Africa.	Mobile internet	25 to 72 hours	Preventive
148.	2015	Meghalaya	Garo Hills	Internet services were blocked in the Garo Hills region for 24 hours to prevent spread of inflammatory messages during the voting period for the Garo Hills Autonomous District Council (GHADC) elections on 11th October, 2015.	Mobile internet	24 hours or less	Preventive
149.	2015	Jammu & Kashmir	Jammu	Jammu experienced suspension of mobile internet services on 8th October, 2015 for around 5 hours to prevent misuse of social media after three carcasses of slaughtered cows were found in the Udhampur area, and the organization of a beef party by an independent MLA	Mobile internet	24 hours or less	Preventive

150.	2014	Gujarat	Godhara	Mobile internet services were shut down as a precautionary measure in the town for 24 hours on the occasion of Ganesh Visarjans, when derogatory messages against Islam started making rounds on Whatsapp on 28th September, 2015	Mobile Internet	24 hours or less	Preventive
151.	2014	Jammu & Kashmir	Entire state of Jammu & Kashmir	Mobile, and wireless internet services were shut down during Eid celebrations on 25th September and 28th September, 2015, apprehending violence against the prohibition on cow slaughter and selling of beef in the State.	Both	73 hours or more	Preventive
152.	2014	Gujarat	Surat	The city of Surat experienced suspension of mobile internet services on 19th September, 2015 as Hardik Patel was detained by the police for violating prohibitory orders against taking out a rally in the area.	Mobile internet	No info	Reactive
153.	2015	Gujarat	Navsari district	From 12th September to 13th September, 2015, mobile internet services were cut off in the district of Navsari, Gujarat in lieu of a march organized by Hardik Patel & his affiliated political organization.	Mobile internet services	24 hours or less	Preventive
154.	2014	Manipur	Entire state of Manipur	Complete internet shut down (mobile and broadband, except for certain BSNL lines) starting 2nd September, 2015 for a week after violence in Churachandpur district.	Both	More than 72 hours	Reactive
155.	2014	Gujarat	Entire state of Gujarat, with prolonged bans in Surat & Ahmedabad	Mobile Internet services shut down in the entire state of Gujarat from 25th August to 2nd September, 2015 after a mega rally led by Hardik Patel seeking OBC status for the Patel community. Mobile internet remained blocked in Ahmedabad & Surat, even post 2nd September, 2015	Mobile Internet	More than 72 hours	Reactive

156.	2014	Jammu & Kashmir	Kashmir	Due to the sudden rise in militant activities in Kashmir, as a preventive measure, mobile internet services were suspended from 8:30 am till 12:00 noon during the Independence Day celebrations in the area on 15th August, 2015. Similar measures are adopted on both, Republic Day & Independence Day in the area every year.	Mobile Internet	24 hours or less	Preventive
157.	2014	Jammu & Kashmir	Jammu	Both, mobile and broadband Internet services were temporarily blocked in Jammu due to the ongoing clashes between the Sikh groups and the state police of Jammu & Kashmir on 5th June, 2015. Although broadband services were restored on 6th June, 2015, there is no information available about the restoration of mobile Internet services.	Both	25 to 72 hours	Reactive
158.	2014	Nagaland	Entire state of Nagaland	Mobile and broadband Internet servies were suspended for 48 hours on 7th March, 2015, after lynching video of a rape accused goes viral.	Both	25 to 72 hours	Reactive
159.	2014	Gujarat	Vadodara	Mobile Internet blocked for three days starting 27th September, 2014 in the city of Vadodara, after riots over a morphed picture of a Muslim religious shrine.	Mobile Internet	25 to 72 hours	Reactive
160.	2014	Jammu & Kashmir	Kashmir Valley	Mobile Internet services were blocked as a part of a security protocol on the occasion of Independence Day on 15th August, 2014. The services were restored within a few hours after the official ceremony was completed.	Mobile Internet	24 hours or less	Preventive

161.	2014	Jammu & Kashmir	Parts of Kashmir	Internet blocked in parts of Kashmir to stop political leaders from addressing a UNHRC event in Geneva via video link on 17th March, 2014. There is no conclusive information available with respect to the restoration of internet services.	Information not available	Info not available	Preventive
162.	2014	Jammu & Kashmir	Few areas in the state	The Defence Ministry had asked the Department of Telecom to selectively ban mobile Internet in some places considered 'hot spots' in the state on 11th March, 2014. There is no information available about the restoration of services in the area.	Mobile internet	No info available	Preventive
163.	2014	Jammu & Kashmir	Most parts of Kashmir	Due to organization of protests at the first death anniversary of Afzal Guru on 9th February, 2014, mobile internet services, and internet through plugged in devices was blocked in most parts of the Kashmir valley as a precautionary measure against apprehended violence till around 5:30 pm on 10th February, 2014.	Mobile internet	25 to 72 hours	Preventive
164.	2014	Jammu & Kashmir	Kashmir Valley	As a precautionary measure on 26th January, 2014, mobile internet, along with mobile telecommunication services was suspended for a few hours.	Mobile internet	24 hours or less	Preventive
165.	2013	Jammu & Kashmir	Entire state	Mobile internet and telephony services were suspended on 15th August, 2013 for security reasons on Independence Day.	Mobile internet	24 hours or less	Preventive

166.	2013	Jammu & Kashmir	Entire state	The entire state experienced a blackout of mobile internet services, lasting almost 5 days, starting 10th August, 2013, due to communal riots that spurred in the Kishtwar district of the state.	Mobile internet	More than 72 hours	Reactive
167.	2013	Jammu & Kashmir	Kashmir Valley	Disconnect of internet services through mobiles & dongles in the Kashmir valley post the killing of four people in the Ramban district after clashes with the Border Security Forces (BSF) on 18th July, 2013.	Mobile internet	No info available	Reactive
168.	2013	Jammu & Kashmir	Entire state of Jammu & Kashmir	TV News channels and mobile Internet banned immediately after Afzal Guru's execution on 9th February, 2013 till 15th February, 2013.	Mobile internet	73 hours or more	Reactive
169.	2013	Jammu & Kashmir	Kashmir Valley	On the occasion of Republic Day, as a part of a security drill, mobile phone and Internet services were suspended on 26th January, 2013.	Mobile internet	24 hours or less	Preventive
170.	2013	Jammu & Kashmir	Kashmir Valley	Mobile internet services were suspended on 21st September 2012 till 5:00 pm owing to the protests over the movie 'Innocence of Muslim's.	Mobile internet	24 hours or less	Reactive
171.	2013	Jammu & Kashmir	Kashmir Valley	Mobile services were suspended on 15th August, 2012 as a precautionary measure for an hour owing to Independence Day.	Mobile internet	24 hours or less	Preventive

172.	2013	Jammu & Kashmir	Kashmir valley	Mobile Internet as a part of a larger mobile telephony ban was restricted on 26th January, 2012 as a standard security protocol.	Mobile internet	24 hours or less	Preventive

Between January 2012 and April 2018, we recorded 172 shutdowns across 19 Indian states, and the number of shutdowns almost doubled every successive year during this period. News reports also provide additional details such as contexts behind shutdowns, types of service affected (mobile/fixed-line), and duration of shutdowns. Based on available information, three groups of preliminary patterns can be made out regarding how Internet shutdowns are imposed:

• Mode of restriction: Whether the order issued restricted mobile, fixed line, or both the modes of connecting to Internet services?

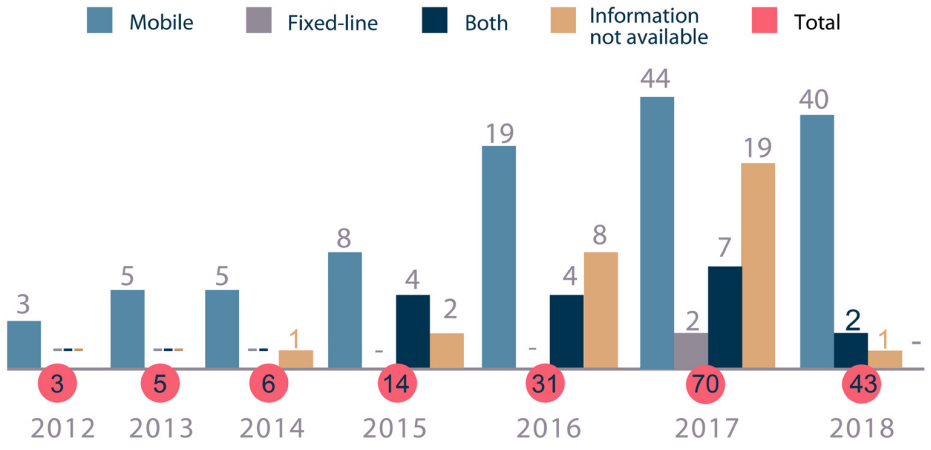
• Duration of the shutdown: Ranging from less than 24 hours to more than 72 hours; how long was the Internet shutdown instituted for?

"Between January 2012 and April 2018, we recorded 172 shutdowns across 19 Indian states, and the number of shutdowns almost doubled every successive year during this period."

• Nature of the shutdown: Was the Internet shutdown a preventive measure taken in apprehension of an event, or as a reaction, post the occurrence?

We emphasize again that the statistics provided here must be treated as purely indicative. Not all news reports provide all the above categories of information every time, and an extent of human error in reportage must also be factored in. Instances where information was unavailable are clearly marked as such.

(Mode of Restriction)



Mode of Restriction

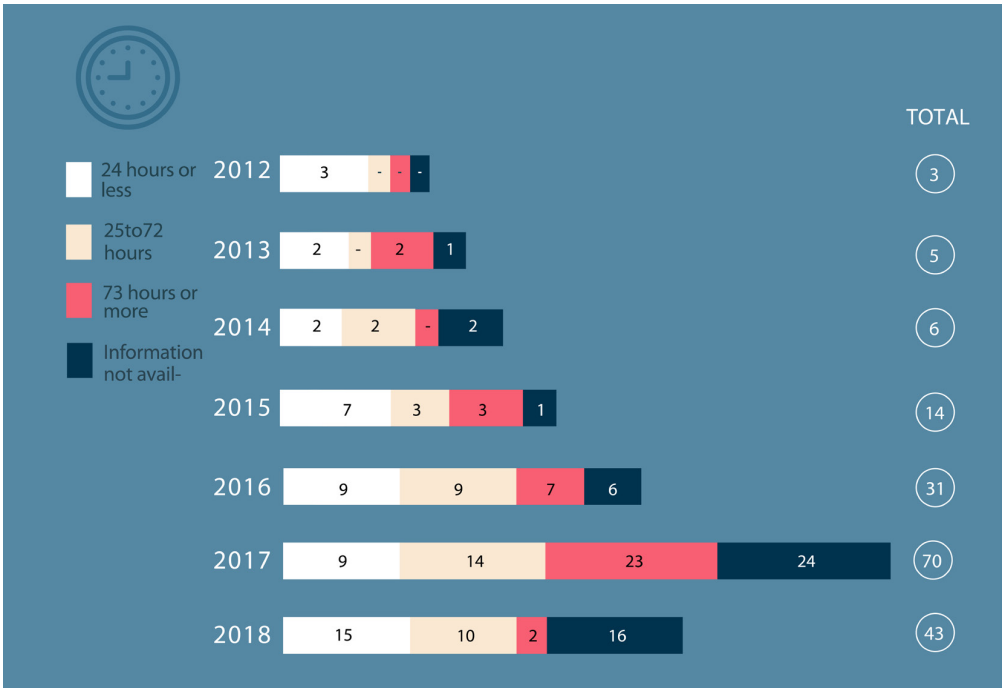
Of the 172 reported incidents, 124 were targeted at mobile Internet services alone (3 in 2012, 5 shutdowns each in 2013 & 2014, 8 in 2015 and 19 in 2016, 44 in 2017 and 40 till April 2018), 17 targeted both mobile and fixed-line Internet services (4 each in 2015 and 2016, 9 in 2017, and 2 in 2018), while only 2 shutdowns targeting fixed-line services alone were recorded during the period of study.

The heavy bias towards targeting mobile networks for shutdowns over fixed-line can be explained by the fact that 95.13% of Indian Internet users access the Internet over mobile networks (phones and dongles), and only 4.87% of Internet users access the Internet using fixed-line services (including wired connections, Wi-Fi, Wi-Max, radio and VSAT)[13]. In other words, of approximately 446 million Internet subscribers in In India, 424 million are mobile Internet users[14].

"The heavy bias towards targeting mobile networks for shutdowns over fixed-line can be explained by the fact that 95.13% of Indian Internet users access the Internet over mobile networks"

These numbers indicate that Government agencies often order mobile Internet shutdowns instead of fixed-line shutdowns because an effective shutdown means preventing maximum number people from accessing the internet to communicate or spread rumours. And since the number

(Duration of Shutdown)



13. Telecom Regulatory Authority of India, *Yearly Performance Indicators of Indian Telecom Sector (Second Edition)*, May 4, 2018, available at: http://trai.gov.in/sites/default/files/YPIRReport04052018.pdf, last accessed on May 4, 2018

14. Ibid.

of mobile Internet users far outnumber fixed-line Internet subscribers in India, restricting mobile internet services is seen as a more effective measure.

Duration of Shutdowns

47 of the 172 Internet shutdowns between 2012 and 2018 lasted less than 24 hours, 38 lasted between 24 and 72 hours, 37 lasted for over 72 hours, while no information was available on the respective durations of 50 Internet shutdowns. The non-availability of information is attributable chiefly to the fact that no public notifications are issued by the Government or Internet Service Providers before, during, or after shutdowns, leaving stakeholders outside affected areas to source this information from available news reports, which do not consistently mention the durations for which Internet access was blocked.

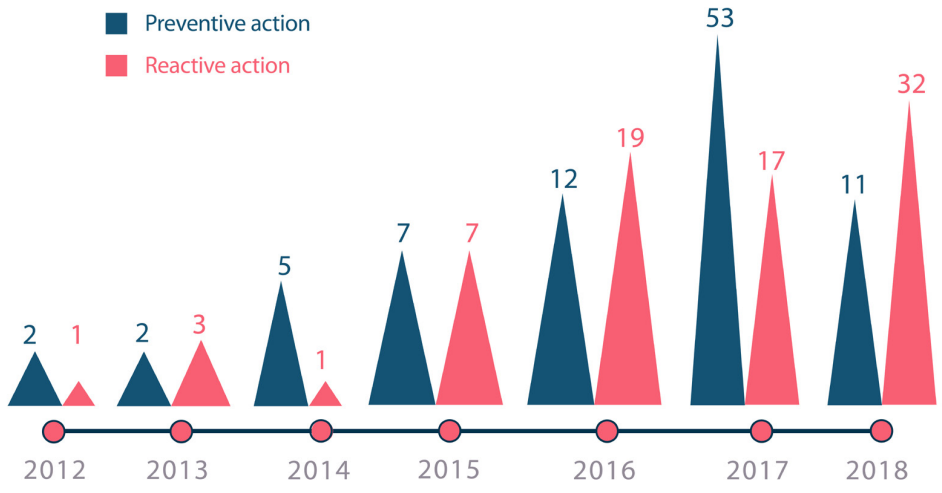
As the above graph reveals, the number of shutdowns lasting over three days has been quickly rising over the years, as has been those lasting between one and three days. Short-duration shutdowns i.e. those lasting less than a day have also been increasing over time, though at a seemingly slower pace. Interestingly, the logest shutdown recorded in India was in the state of Jammu and Kashmir, where Internet services remained suspended for almost 6 consecutive months.

Nature of Shutdowns

Of the 172 Internet shutdowns recorded between January 2012 and April 2018, 92 were observed to be preventive measures i.e. restrictions imposed in anticipation of law and order breakdowns, whereas 80 shutdowns were reactive in nature i.e. imposed in order to contain on-going law and order breakdowns.

It is especially interesting to note that the number of preventive shutdowns often match and at times surpass the number of reactive shutdowns overall. In 2017, the number of preventive shutdowns were almost three times the number of reactive shutdowns, indicating that Internet shutdowns are increasingly being resorted to even before law and order breakdowns have actually taken place.

(Nature of Shutdown)



CHAPTER 5

Voices of the affected

Over the last decade, Internet has become an essential utility to facilitate activities of all kinds including but not limited to communications, business, education, health and journalism. In order to gain a better understanding of how Internet shutdowns impact the daily lives of residents, we reached out to people across the nation to pen down their experiences during the times of Internet shutdowns. Following is a collection of brief quotes we received from those affected by Internet shutdowns, explaining how Internet shutdowns have affected them and others they know.

Impact on Business & Economy

A report[15] by the Brookings Institute, which aimed to quantify the losses suffered by various countries due to such internet, adjudged India to have topped the list by incurring losses to the tune of US $968 million in the year 2016 itself. To measure national Internet shutdown costs, Brookings used the following formula: [national GDP * duration (measured as percent of the year based on number of days the Internet was shut down) * extent of digital economy (measured as percent of national economy derived from the digital economy) + the multiplier effect of the disrupted digital economy]. Another report[16] by the Indian Council for Research on International Economic Relations, which quantatitavely assessed the economic impact of Internet Shutdowns across India, projects an economic loss of approximately US $3.04 billion due to Shutdowns in the country during the period of 2012-17. To determine economic impact of shutdowns, ICRIER relied on the estimated elasticities of mobile and total Internet in combination with the estimated economic cost of Internet traffic affected by shutdowns. Yet another report prepared by Deloitte and launched by the Global Network Initiative, found that an average high-connectivity country stands to lose at least 1.9% of its daily GDP for each day all Internet services are shut down. For an average medium-level connectivity country, the loss was estimated at 1% of daily GDP, and for an average low-connectivity country, the loss was estimated at 0.4% of daily GDP[17]. All of these reports convey that with the growing dependence on online ecosystem, the economic impact of internet shutdowns has also magnified.

“All of these reports convey that with the growing dependence on online ecosystem, the economic impact of internet shutdowns has also magnified.”

With the Digital India campaign, businesses are rapidly adopting online business models, where Internet disruptions for even a few hours brings

15. Darrell M West, *Internet shutdowns cost countries $2.4 billion last year,* Center for Technology and Innovation at Brookings, https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf, October 2016

16. Rajat Kathuria, Mansi Kedia, Gangesh Varma, Kaushambi Bagchi, Rekha Sekhani, The Anatomy of an INTERNET BLACKOUT: Measuring the Economic Impact of Internet Shutdowns in India, ICRIER, http://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf, April 2018.

17. Deloitte, *The Economic Impact of Disruptions to Internet Connectivity,* October 2016, available at: https://globalnetworkinitiative.org/

the business to a halt due to breakdown of communication channels with their potential customers, payment gateway operators, delivery personnel and other such intermediary parties involved.

Dipak Birolia, cotton bales trader in Adilabad town in state of Telangana expressed his concerns about how the long term Internet Shutdown affected his export business. He struggled to keep his business running, he had to travel 40 kms every day to access internet and generate E-way bills to ensure transportation of his goods. He said, *"We faced a lot of problems when there was no internet in our region for more than a month. We have an export business that requires the filing of various bills etc. Since there was no internet, we couldn't generate E-way bills for transportation of goods. We used to go 40 km every day to Maharashtra in order to access the internet and complete our work. This was only once, but after that, we haven't faced any problem." - Dipak Birolia, cotton bales trader in Adilabad town.*

There are certain businesses that run only through the Internet. E-commerce websites, websites for job procurement, e-trading, e-banking applications are among the few business models for which Internet is essential and is absolutely necessary to facilitate services to customers/subscriberes. Internet disruptions affect their entire economic existence.

Sairee Chahal, Founder & CEO, of SHEROES, told us about her online platform which aids women across the nation from diverse background in finding jobs. She expressed her concerns during the time of network disruption as, *"SHEROES works with women from over 20,000 locations and internet shutdowns have adversely impacted our daily business. Internet serves as a lifeline for income for many and shutdowns change that negatively".* The impact of shutdown is not limited to big traders, E-commerce, or big companies but an Internet blackout tends to equally impact even the smallest business which has any form of Internet dependence. An operator at a service center from Mutnur village of Adilabad district narrated his experience to us. According to him, *"Various business areas suffered when there was no internet for 30-45 days in our region. Our work includes filling of online applications, generating certificates like birth certificate, OBC certificate etc. Since we couldn't do any bank transactions, our customers also faced a lot of inconveniences."*

Impact on Human Rights

Internet disruptions have a direct impact on human rights and the same has been acknowledged by the Special Rapporteur's June 2017 Report to the Human Rights Council which states that the users affected from an Internet shutdown are cut off from emergency services and health information, mobile banking and e-commerce, transportation, school classes, voting and election monitoring, reporting on major crises and events, and human rights investigations.

In addition, a resolution[18] was passed by the United Nations Human Rights Council on 1st July 2016, condemning network disruptions and measures resorted by states to curb online access and/or dissemination of information. The resolution further affirmed that rights in the online sphere, especially the right to freedom of expression requires the same standard of protection as in the offline world. It recognized the role of Internet in promoting affordable educational opportunities.

The general population of India agrees with

18. United Nations, General Assembly, Human Rights Council, *Promotion and protection of all human rights, civil,political, economic, social and cultural rights, including the right to development.*, Thirty-second session, Agenda item 3, 27th June 2016

the views cited by United Nations with respect to human rights violation caused by network disruptions. Faizal Farooqui, CEO of Mouthshut.com, expressed that, *"Internet shutdowns are a violation of the Constitutional Right to Freedom of Speech and Expression. They cause damage to the economy, individuals and businesses. They also cause longterm harm to the people of affected regions by denying them access to knowledge".*

Burhaan Kinu, Sr. Photojournalist, Hindustan Times had similar concerns as Mr. Farooqui, he said that, *"curbing Internet services violates basic human rights and does irreversible economic and social damage to common citizens of the state".*

In addition, a homemaker, Anuradha Devi also gave a detailed account on how Internet disruptions have affected her daily life. While there was a 100 day internet blackout in Darjeeling, she realized the importance of the Internet, she felt isolated from the community and felt a forceful disconnect from the rest of the world.

In her words, *"Earlier, I was using the Internet for the sole purpose of being active on social networking. However, the Internet Shutdown in Darjeeling made me realize the actual importance of the Internet and pointed my attention towards the fact that how important it has become for us to get information about the world and be connected with each other. Not only we were cut-off from the outside world but there was no way we could reach them and tell our condition".*

> **"As I passed my class 12 exams, I was thinking of pursuing law but could not even apply for the course as there were no Internet services. Even the mobile networks kept on fluctuating which made it difficult to get any kind of updates on admissions and otherwise."**

> **"The Internet Shutdown in Darjeeling made me realize the actual importance of the Internet and pointed my attention towards the fact that how important it has become for us to get information about the world and be connected with each other. Not only we were cut-off from the outside world but there was no way we could reach them and tell our condition".**

Impact on Education

An Internet shutdown is more than just a disconnection from Whatsapp, Facebook or Twitter; it means limiting access to knowledge and learning opportunities for students. It also leads to restriction from avenues for learning that are provided by platforms like Coursera or edX. During an Internet shutdown, students are bereft of access to information, education programs, fellowships among other educational activities.

Geeta Devi, a class XIIth student from Darjeeling spoke to us about the difficulties she and peers faced in the application process for their college admissions during a sixty four day Internet Shutdown in Darjeeling. It was a crucial time for all the newly school graduates to apply for their higher studies, but due to lack of proper internet services they failed to recieve everyday updates on admissions. As a result, Geeta missed the deadline and couldn't apply for the course she desired to pursue. She says, *"The 64 days long Internet shutdown in Darjeeling started in*

the month of July, that was the time when admissions in most of the colleges and universities begin. As I passed my class 12 exams, I was thinking of pursuing law but could not even apply for the course as there were no Internet services. Even the mobile networks kept on fluctuating which made it difficult to get any kind of updates on admissions and otherwise. I am not the only one who is suffering, all the students in Darjeeling are facing similar issues."

Psychological impact

When Internet services suddenly become unavailable at a time when so many aspects of our lives are dependent on it, the impact can be felt not just economically but also psychologically. Saadia Ishfaq, a Community Manager, Srinagar, Jammu & Kashmir told us that she felt like as if she was being strangulated. *"Life came to a standstill. Snapping of Internet services was the biggest blow. There was no communication at all. One couldn't reach out to anybody."*

Another eleventh grader from Darjeeling, Ayush Chaurasia, reported his experience during a month long Internet Shutdown in the city. Internet shutdowns are a hindrance to the ability of children to research and study. In addition, the impact of shutdowns is not limited to their education but it also affects psychology of children since the shutdown leaves a child disconnected from the rest of her peer group.

"It has been over two months. I haven't gone to school. All the schools in Darjeeling are closed due to persistent upheaval and chaos. As far as the internet is concerned, I am unable to access any kind of information. I used to continuously visit many online portals for my research work but now I cannot even study a small piece of information as there is no internet. I cannot connect to my friends and there is no exchange of any kind of information due to internet shutdown."

Impact on health industry

Internet is an indispensable utility service for health care industry. Most of patient information repositories, documentations and records are maintained on online servers. At the time of an Internet shutdown, it becomes impossible to work on these servers. In addition, doctors often consult their peers in complicated cases for advice, and with the advent of the Internet and messaging services like WhatsApp, communications have become easier through images and videos. However, Internet shutdowns prevent them from communicating with their peers and experts virtually.

"Most hospitals host their databases on servers online. Also, various life saving drugs and surgical instruments are shipped to us from across the world. Ordering, making payments and subsequent tracking of shipment—all happen online. With the Internet shutdown, we needed to improvise with a contingency plan since we didn't have access to detailed patients' information."

Dr. Regina Rajkumari, Surgeon, a native of Manipur, recited her experience from an Internet Shutdown, *"Most hospitals host their databases on servers online. Also, various life saving drugs and surgical instruments are shipped to us from across the world. Ordering, making payments and subsequent tracking of shipment—all happen online. With the Internet shutdown, we needed to improvise with a contingency plan since we didn't have access to detailed patients' information."*

CHAPTER 6

Conclusion

Over the previous sections of this report, we have seen how Internet shutdowns developed as a state response to law and order situations and how existing legal frameworks govern their imposition. We have had a look at all the shutdowns that have been recorded in India since January 2012 and identified a few key patterns that emerge from available data. We have also heard from individuals who were directly or indirectly affected by Internet shutdowns, and heard first-hand accounts of how recurring Internet shutdowns deal a heavy blow to socio-economic welfare and growth. As Internet shutdowns continue to gain favor with the Government as an effective way to control the spread of rumors and misinformation during imminent/existing law and order breakdowns, it is safe to say that this is one of the most pressing public policy issues in the contemporary landscape.

A number of actors in the multi-stakeholder community have also taken cognizance of the urgency of this issue and joined the narrative against Internet shutdowns. In India, various civil society organizations, academic institutions, and policy think tanks have published research reports on Internet shutdowns. Other stakeholders like media organizations and industry stakeholders routinely participate in the discourse in some capacity by organizing and speaking at various events and consultations. Even Government officials have infrequently participated in policy discussions on Internet shutdowns, though their narratives have mostly focused on how shutdowns solve a real security concern and how there are no other viable alternatives.

On the international plane, there are even more organizations that have already dedicated a great deal of resources to studying and fighting Internet shutdowns. For instance, Access Now – a global civil society organization headquartered in the United States spearheads the #KeepItOn campaign with a dedicated website that provides a vast array of information material including contributions from a number of partner organizations across the world. Other stakeholders like the Internet Society, Global Network Initiative, Brookings Institution and even the United Nations have all weighed in on the issue of Internet shutdowns. The United Nations Special Rapporteur on the Protection and Promotion of Freedom of Expression and Opinion has in fact issued several calls to end Internet shutdowns to countries where they are common, including India.

“As the narrative against Internet shutdowns gains momentum on a global level, India stands out as a shining example for all the wrong reasons. With at least 172 shutdowns recorded between January 2012 and April 2018, India has the distinction of being home to the highest number of shutdowns recorded anywhere in the world, that too by a wide margin.”

As the narrative against Internet shutdowns gains momentum on a global level, India stands out as a shining example for all the

wrong reasons. With at least 172 shutdowns recorded between January 2012 and April 2018, India has the distinction of being home to the highest number of shutdowns recorded anywhere in the world, that too by a wide margin. According to Access Now, which also runs a Shutdowns Tracker on a global scale, India in September 2017 topped the list of 30 countries that witnessed shutdowns in the preceding 21 months.

This is a very curious state of affairs, as the Government of India's flagship initiative Digital India places great emphasis on the Internet and technology in general to carry the country to the next phases of its development trajectory. The Government strong push for digitalization is also visible in projects like the Aadhaar unique ID program, which seeks to create a central database of demographic and biometric information on Indian residents so as to streamline governance and public life in many ways. This and other programs like smart cities and the Internet of Things all have one thing in common i.e. none can function without reliable access to the Internet at all times. Considering the importance that India places on the Internet in furthering its development goals, it is highly counterintuitive that it has also made a habit of shutting down Internet access during law and order situations, ignoring the obvious and severe collateral damage that such measures come with.

On the other hand, it cannot be ignored that the Internet has indeed presented a range of fresh challenges when it comes to containing law and order breakdowns. The ease with which rumors and misinformation can be circulated online to reach a very large audience, the opportunities the Internet presents for discreet planning and execution of malicious efforts meant to disrupt peace and tranquility, and even features like encrypted communications that are considered indispensable to ensure privacy and security but which also benefits malicious actors, all contribute in equal measure towards making it that much more difficult for law enforcement agencies to prevent/mitigate law and order breakdowns and limit destruction and injuries during turbulent times. All things considered, it is not difficult to see how Internet shutdowns would seem to the authorities to be an attractive way of tackling law and order breakdowns, but it is truly unfortunate that this excessive measure is being wantonly resorted to with little to no consideration of how they might impact societies and economies in the long run.

"On the other hand, it cannot be ignored that the Internet has indeed presented a range of fresh challenges when it comes to containing law and order breakdowns."

To address the issue of Internet shutdowns in an effective and balanced way, a number of short and long term steps must be collectively taken by the multi-stakeholder community:

- The current legal regime governing Internet shutdowns must be overhauled to place greater emphasis on transparency and accountability. The Temporary Suspension of Telecom Services (Public Emergency and Public Safety) Rules, 2017 must become the only legislation under which Internet shutdowns are imposed. This by extension means shutdowns must no longer be imposed under Section 144 of the Criminal Procedure Code, which is not designed to facilitate carefully considered shutdowns with adequate oversight. The Telecom Suspension Rules must

be treated as the procedure governing shutdowns imposed under Section 5(2) of the Telegraph Act, and all shutdown orders issued under Section 5(2) must abide by the procedure laid out under the Telecom Suspension Rules.

- The Telecom Suspension Rules themselves must be updated with language that requires issuing authorities to exhaust all available alternatives before issuing an Internet shutdown order. Moreover, the Rules must make it necessary to provide adequate notice to the general public before Internet shutdowns are imposed, clearly specifying the duration for which each shutdown is expected to remain in place. Any extensions of existing shutdowns must also be similarly notified. The act of issuing notices may be carried out by TSPs, and issuing authorities must be empowered to issue necessary directions in this regard. Further, the Rules must introduce provisions that require Government agencies to make Internet shutdown orders publicly accessible, and catalogs of all such orders issued so far must also be maintained and made public accessible. Statistics must also be made available on how often the Review Committee meets and the decisions taken at these meetings.

- The multi-stakeholder community must work together to undertake a study of the actual impact of the Internet on spreading rumors and misinformation before, during and after law and order breakdowns. Specifically, the study must attempt to answer at least the following questions:

  - Is there a consistent and perceptible increase in the dissemination of rumors and misinformation before, during and after law and order breakdowns?

  - Is there a causal link between rumor-mongering online and escalations in real-world law and order problems?

  Lack of adequate research in this regard is what stalls most dialogues with the Government on addressing Internet shutdowns, as any calls to end Internet shutdowns are easily countered by the authorities with the insufficiently proven argument that shutdowns save lives by preventing rumor-driven escalations of law and order problems. Depending on the outcome of the study, the multi-stakeholder community must also work together to conceptualize viable alternatives to Internet shutdowns that balance the interests of all stakeholders.

> **“Filling in research gaps and conceptualizing solutions is not something that actors in this space can perform in isolation, which means meaningful collaborations and focused dialogues are indispensable.”**

As evident from the above, the campaign against Internet shutdowns is still in its nascent stages, and there is much ground to be covered before the issue can be effectively addressed. Filling in research gaps and conceptualizing solutions is not something that actors in this space can perform in isolation, which means meaningful collaborations and focused dialogues are indispensable in arriving at an expedient solution. We hope that this report is of use to those looking to enter the debate around Internet shutdowns as well as those already in it, and we look forward to working with the community to ensure that the Internet remains a driving force behind sustainable growth.

sflc.in

About Us

SFLC.IN is a donor supported legal services organization that brings together lawyers, policy analysts, technologists, and students to protect freedom in the digital world. We promote innovation and open access to knowledge by helping developers make great Free and Open Source Software, protect privacy and civil liberties of citizens in the digital world through education and provision of pro bono legal advice, and help policy makers make informed and just decisions with the use and adoption of technology. Please feel free to contact us to learn more about protecting your rights in the online world.

Living in Digital Darkness

A handbook on internet shutdowns in India

K 9, Birbal Road, Second Floor,
Jangpura Extension, New Delhi 110014, India
Tel: +91-11-43587126, Fax: +91-11-24320809
www.sflc.in

Chapter 27

OpenChain Announces Partner in India
(Shane Coughlan)

OpenChain Announces Partner in India

By Shane Coughlan April 17, 2019 News

- https://www.openchainproject.org/news/2019/04/17/openchain-announces-partner-in-india

The OpenChain Project is delighted to announce our first law firm partner in India. From today you will be able to obtain legal advice about OpenChain Conformance and other OpenChain matters from *Mishi Choudhary & Associates* LLP. We look forward to building a long-term relationship with Mishi Choudhary and her team.

Learn More About Mishi Choudhary & Associates LLP

- https://mcalaw.in/

Chapter 28

GPL-3.0 in the Chinese Intellectual Property Court in Beijing (Lucien C.H. Lin and Navia Shen)

GPL-3.0 in the Chinese Intellectual Property Court in Beijing

Lucien C.H. Lin,[a] Navia Shen,[b]

(a) Legal Adviser, Open Culture Foundation; (b) IP Counsel, Huawei Technologies Co., Ltd.

DOI: 10.5033/ifosslr.v10i1.126

Abstract
With the increasing use of Free and Open Source Software (FOSS) in the world, the licensing issues and disputes regarding such licenses have been litigated in various jurisdictions. In the past, these lawsuits were concentrated in Europe and the United States, but less so in the Asia Pacific region. However, in 2018, the specialized Intellectual Property Right Court in Beijing, China, acting as a court of first instance, issued a decision in a software copyright infringement lawsuit related to FOSS. The defendant chose to invoke the copyleft mechanism in the GNU General Public License 3.0 (GPL-3.0) license as a defense against claims of copyright infringement. Although the court did not directly interpret the GPL license at this stage, the decision strongly implies that the GPL and the other FOSS licenses can be treated as valid in China. Even so, quite a number of details regarding the use of the GPL in China still require clarification, included as to how the license can substantially be enforced and implemented.

Keywords
Copyleft, GPL, derivative work, copyright infringement

Although most of the academic opinions are positive,[1] many commentators and practitioners did have doubts about whether a Free and Open Source Software license written in English could be enforced legally in China. After all, in 2014 the China Open Source Software Promotion Union (COPU)[2] once published a draft of "COPU Open Source General License Agreement V.1.0".[3] The text of COPU 1.0 was written purely in Simplified Chinese language and was meant to be used as an alternative solution in China for Chinese Free and Open Source Software projects. The COPU 1.0 actually was not used in any released Free and Open Source Software project due to the resource limitation for project development, and this license lasted only at the stage of public comments. However, the draft and publication of the COPU 1.0 reflected concerns as to whether Free and Open Source Software licenses written in foreign languages could be enforced in full in China without

1 As discussed in YANG XIA, *Introduction to Software Protection under Chinese Law*, http://ifosslawbook.org/china/, Section "Analysis of FOSS Under China Law".
2 http://www.copu.org.cn/about [retrieved June 2018]
3 https://www.oschina.net/news/52060/coup-license-comment [retrieved June 2018]

obstacles. Back to 1991, it was stipulated in the "China Regulation on Computers Software Protection", article 18, that in the case of a license to exploit software copyright, the license shall be made in formality according to the related laws and regulations of the China government. This requirement for formality has been removed in the revised version of the regulation, however some people still have doubt that whether or not a software license or contract not written in Simplified Chinese language could be fully applied in disputes during trial proceedings. This doubt was one of the reasons that the COPU group, supported by the China government industrial administration departments, tried to to prepare a new FOSS license suite purely written in Simplified Chinese on their promotion activities. This doubt remained, but now it seems to have been answered in the recent case of DCloud vs APICloud.[4] The plaintiff in this lawsuit is Digital Paradise (Beijing) Network Technology Co., Ltd. (DCloud), and the defendants are Pomelo (Beijing) Technology CO., LTD. & Pomelo (Beijing) Mobile Technology CO., LTD. (APICloud). The case, involving civil software infringement litigation, was filed in 2015 and a decision was handed down in April 2018. In this lawsuit, the GNU General Public License version 3 (GPL-3.0), especially the copyleft mechanism in it, was reviewed by the trial judges of the trial bench. The decision of the court affirmed the enforceability of the license.

Plaintiff's Claim

The plaintiff DCloud asserted that in September 2014 the defendant APICloud copied and adapted three independent plug-ins of plaintiff's HBuilder software development kit into the defendant's released APICloud toolset. The registered names of the allegedly infringed plug-ins in order in National Copyright Administration of China were "CIM plug-in", "ACR plug-in", and "HTML code drawing in real time plug-in". The plaintiff alleged it was the copyright owner of the HBuilder software, and that HBuilder was developed and largely released as shareware for limited use at no charge. While some of the modules and plug-ins in the HBuilder project were provided under certain FOSS licenses, including the GPL, these three allegedly infringed plug-ins were independent software works not provided under FOSS license. As such, the allegedly unauthorized copying and distribution of these three plug-ins infringed the right of reproduction, the right of alteration, and the right of information network dissemination protected under Article 9[5] of the Copyright Law of the People's Republic of China (2010 Amendment). Based on that, the plaintiff sued for the judgment of the court, demanding that the defendants publish an apology statement on its website www.apicloud.com and also on the other appointed information platforms for one month. Other than that, plaintiff also demanded RMB 3.5 million as compensation for copyright infringement, economic losses and legal costs.

Defendants' Defense

The defense of Pomelo (Beijing) Technology CO., LTD. & Pomelo (Beijing) Mobile Technology CO., LTD. (APICloud), as the defendants, was that part of the modules and plug-ins in the HBuilder project released by the plaintiff were derived from previously existing GPL-3.0-licensed components, such as "Aptana"[6] originally developed by Appcelerator, INC. under GPL-3.0 as a module in the Eclipse framework. Therefore, HBuilder project should be considered open source software made available under the GPL-3.0 license, and anyone has the right to use the code and create derivative works based on it under the terms of the GPL 3.0 license. Under this understanding of GPL-3.0, defendants asserted that plaintiff's consent was not required to use parts of the source codes from the HBuilder project for the APICloud project, and this kind of usages of software licensed under GPL-

4 (2015) 京知民初字第 631 号 / (2015) Jingzhi MinchuZi No. 631 of 22/03/2010 http://www.bjcourt.gov.cn/cpws/paperView.htm?id=100734294859&n=1 [retrieved Jan. 2019]
5 http://www.lawinfochina.com/Display.aspx?lib=law&Cgid=127326#menu1
6 https://github.com/aptana/studio3

3.0 should not constitute infringement of copyright. In addition, even if the disputed activities constituted infringement, the compensation requests have no facts or legal basis: APICloud project and DCloud project are both provided for free, the three disputed plug-ins are not core software of plaintiff, only minor parts of DCloud project are used, and defendants exhibited no subjective malice. Moreover, defendants asserted that there was no legal basis to demand publication of an apology statement. On account of the reasons above, the defendants requested that the court dismiss the plaintiff's claim.

Court Forensics and Judgement

The facts and legal judgements of the court in this case focus on copyright substantial similarity and forensics determining the relationship between the software. The identification task was entrusted to the Judicial Authentication Institute for IP Rights of CSIP.[7] Based on its analysis, the Authentication Institute reported:

> *On the first phase of the identification work required by the claimant, between the source codes of HBuilder and APICloud on plug-ins with the same or similar functions, for the CIM plug-in, there are 29 of the 30 source code files in the APICloud project being identified as substantially similar to the HBuilder project. For the ACR plug-in, 18 of the 23, and for the HTML code drawing in real time plug-in, 44 of the 56.*
>
> *Then on the second phase of the identification required by the defendants, the source code files found similar between HBuilder and APICloud, once more were verified with the third party's and Free and Open Source Software components prior to the release date of HBuilder provided by the defendants, for the CIM plug-in, there is none of the 29 source code files being identified as substantially similar to the previous Free and Open Source Software components. For the ACR plug-in, 13 of the 18, and for the HTML code drawing in real time plug-in, 2 of the 44.*

In accordance with the reports of the forensics above, given that 13 of the 18 between the ACR plug-in and the Free and Open Source Software components are similar, one might argue the GPL derivative issue for the ACR plug-in can be studied further, however, the judges of the trial bench ruled in the written judgment that "Of the aforementioned source code of similarity, only a small part of the source code is the same as the third-party or Open Source Software provided by the defendants." Hence, the conclusion by the court (discussed further below) is that the three plug-ins in dispute are independent copyrighted works of plaintiff, not derivative works of GPL-licensed software, the court of trial held that defendant infringed plaintiff's right of reproduction, the right of alteration, and the right of information network dissemination protected by the Copyright Law of the People's Republic of China. Therefore, the court ruled that the copyright infringement shall be compensated in the amount of RMB 1.25 million in economic losses and RMB 39,480 in lawsuit costs.

The Crucial Point

The crucial point of this lawsuit is that the defendants have proposed the copyleft mechanism in the GPL-3.0 as their primary defense method by claiming that the HBuilder project as a whole should be made publicly available under the GPL-3.0 license, and also alleged that their modification from the HBuilder project to the APICloud project are lawful acts permitted by the GPL-3.0 license. As for the GPL-3.0, the court of trial did not, in principle, deny the validity of it as a license agreement

7 Judicial Authentication Institute for Intellectual Property Rights at China National Software and Integrated Circuit Promotion Center (CSIP) of Ministry of Industry and Information Technology, at: http://www.csipsfjd.org.cn/

during the whole trial process. The court even introduced many paragraphs of the GPL-3.0 license in the written judgment for the factual section, for example, these contents of the GPL-3.0 have been translated into Chinese and quoted in the legal reasoning:

> *0. Definitions.*
>
> *"The Program" refers to any copyrightable work licensed under this License.*
>
> *[...]*
>
> *To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.*
>
> *5. Conveying Modified Source Versions.*
>
> *You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:*
>
> *[...]*
>
> *c) [...] This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged [...]*
>
> *d) [...]*
>
> *A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.*

Overall, the court of trial supported the validity and enforceability of the terms of GPL-3.0 and seemed to be willing to issue a decision based on the relevant provisions of the GPL-3.0. The main reasons presented by the court of trial in the written judgement are:

1. Based on the two identification results, the three plug-ins in dispute among HBuilder project and APICloud project do have quite a number of similarity issues of source code citation and modification, and only small parts of those similar source code have similarity issues with previous third party and other Free and Open Source Software. And for that reason, the court held that APICloud has copied and modified those plug-ins of HBuilder project for defendant's APICloud project.

2. Based on the copyright registration certificates for those three plug-ins, and plaintiff's explanation, the court held that plaintiff is the copyright owner of those three plug-ins, and those three plug-ins are separate and independent works and can be executed independently. This finding was based on

the fact that there is no GPL license text in the subdirectories of the three plug-ins or in the root directory of the HBuilder project. Although one other subdirectory of HBuilder contains GPL license text, the court held that that license text does not apply to the three plug-ins in dispute. Furthermore, the court held that all the three plug-ins are not derivative works or modifications referred to in the GPL license, which would have required the source code of the plugins to be made available publicly under the GPL license.

3. Based on above 1 and 2, the court further held that defendants' defense that Claimant's software shall be Free and Open Source Software was not supported. As such, the court held that defendants infringed copyright owner's rights of copying, adaptation and information network dissemination.

Judging from the grounds of judgement above, this decision made in this first instance can still be reasonably appealed to a higher court. However, if the defendants can't substantiate that the three plug-ins in disputes are derivative works of GPL licensed software rather than independent works, such as by deeply analyzing the interaction relationship between the GPL licensed parts and the other parts, including the three plug-ins in dispute, as well to assert that license text is not attached doesn't avoid corresponding codes for the derivative works to be made available publicly under GPL license. Even if the appeal is allowed, the defendants still have much to do to turn the tide in the followed proceedings. Usually the rulings of the Beijing IPR court are based on the reliance and respect for the forensics made by the CSIP. That means if APICloud can't make a credible argument regarding the copyleft effect for the appeal, both in legal inference and technical analysis for explaining why the original judgment is in contravention of the laws and regulations, their appeal might be treated as meritless and not favored by the trial court on appeal. Still, if those evidences are successfully substantiated, it will make the appeal case to be very complicated, as the court would be required to determine what constitutes a derivative work under GPL license and, if software is considered a derivative work of GPL-licensed software, then whether or not the defendants can directly procure and use these source codes under GPL license without additional permission of the Claimant as they asserted, and whether the defendants can require the Claimants to provide the related source code under the GPL.

According to the online article[8] published by the plaintiff's attorney in this case, although the defendants proposed to invoke the copyleft mechanism of GPL-3.0 as its defense, the arguments of the APICloud group were weak and not persuasive. That is, the defendants neither can explain what is their interpretation for the copyleft mechanism of GPL-3.0 in detail, nor can respond properly to the distinction between covered work as a whole and aggregation as separate parts in a compilation solution proposed by the plaintiff. In brief, assuming that the Hbuilder software contained some GPL 3.0 software, the court could either have viewed the Hbuilder software as subject to the GPL 3.0 license as a whole or instead as an aggregate not subject to the GPL 3.0 license. In this lawsuit, since the involved plug-ins are treated as separate works not based on prior GPL 3.0 software according to the entrusted forensics, the burden of persuasion fell upon the defendants, and the defendants failed to persuade the judges in court their way is the right way to do the copyleft interpretation, the judges made the final decision on the side of the plaintiff.

In Conclusion

In comparison with other international Free and Open Source Software litigation, this verdict does not provide much further analyses and in-depth explanations of how the Free and Open Source Software licenses should be evaluated and enforced in judicial proceedings. However, from a symbolic point of view, this case does have the value of being recorded and tracked. The main

8 *Will your cheese be taken away on account of Open Source licenses? - The constitution of copyright infringement of computer software involving open source licenses*: http://www.unitalen.com.cn/html/report/18040838-1.htm [retrieved June 2018]

reason is that the Beijing Intellectual Property Right Court is a specialized court in the intellectual property right field, the presiding judge and the other two People's Assessors in this trial, comfortably showing their support for the validity of GPL-3.0 without raising any doubt or objection. The disputed plug-ins in this ruling such as CIM plug-in, ACR plug-in, and HTML code drawing plug-in alledged as copyright infringements by the plaintiff are deemed to have no copyleft issues based on the CSIP forensics in the conclusion. However, because the defendants claimed the copyleft mechanism as their defense in the early stage, for the first time, the differences between a “covered work” and an “aggregate” for the Modified Versions of the Programs licensed under GPL-3.0 have been introduced by the Beijing IPR court. This lawsuit can be regarded as the beginning of judicial interpretation of Free and Open Source Software licenses in China.

As a matter of fact, the APICloud group, as the defendants of this case, have already made a positive statement[9] that they are appealing to the higher court for the second instance. In this statement, the APICloud group did admit that due to the lack of due diligence, back to 2015, when part of the plug-in codes from the HBuilder project were imported into the APICloud project, they didn't do it very well on filtering out the third party modules with no Free and Open Source licensing notice. However, after the dispute occurred and was notified by the DCloud in the same year, they subsequently released a new version of the APICloud project, which all has been licensed under GPL-3.0, and provided publicly to anyone on the hosting page of APICloud project onto GitHub[10]. By now, the APICloud group still believe that on account of the application and interaction method to the original GPL-3.0 modules in the HBuilder, the HBuilder project as a whole should be made available under GPL-3.0 without a difference. Therefore, more distinction and clarification for the covered scope of GPL-3.0 in the scenario of derivative or adaptation will likely be further discussed in the legal proceedings to come, and the subsequent effects and impact are worthy of continuous observation.

About the authors

Lucien Cheng-hsia Lin*, legal adviser both of Open Culture Foundation and Gemly Int'l Intellectual Property Right Office, has been participating in the Open Source, Open Data, and Creative Commons Licenses interpretation and clarification among the local communities, official agencies, and companies in Taiwan for more than 10 years. He is best known for being the main proposer and drafter of the "Open Government Data License Taiwan 1.0" (https://data.gov.tw/license), with an one-way CC BY 4.0 switching mechanism implemented, which can make most of the materials on Taiwan Open Data portal available under CC BY 4.0 license.*

Navia Shen*, legal counsel of Huawei Technologies Co., Ltd, has been working in Huawei for copyright and open source related affairs for about ten years.*

9 https://community.apicloud.com/bbs/thread-86486-1-1.html [retrieved June 2018]
10 https://github.com/apicloudcom/APICloud-Studio [retrieved June 2018]

Chapter 29

15 CFR 744: Additions to Entity List

122°48′28″ W; to lat. 46°56′44″ N, long. 122°47′08″ W; to lat. 46°55′28″ N, long. 122°47′10″ W; to lat. 46°54′42″ N, long. 122°47′45″ W; to lat. 46°55′28″ N, long. 122°49′51″ W; thence counter-clockwise along the 4-mile radius of the airport to the point of beginning.

Paragraph 6005 Class E Airspace Areas Extending Upward From 700 Feet or More Above the Surface of the Earth.

* * * * *

ANM WA E5 Olympia, WA [New]

Olympia Regional Airport, WA
(Lat. 46°58′10″ N, long. 122°54′09″ W)

That airspace extending upward from 700 feet above the surface within a 6.8-mile radius of Olympia Regional Airport from the airport 211° bearing clockwise to the airport 088° bearing, and within an 8.2-mile radius of the airport from the airport 088° bearing clockwise to the airport 122° bearing, and within a 12.4-mile radius of the airport from the airport 122° bearing clockwise to the airport 211° bearing, and within 1 mile each side of the 011° bearing from the airport extending to 11.6 miles north of the airport.

Issued in Seattle, Washington, on May 8, 2019.

Shawn M. Kozica,

Group Manager, Operations Support Group, Western Service Center.

[FR Doc. 2019–10554 Filed 5–20–19; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Part 744

[Docket No. 190513445–9445–01]

RIN 0694–AH86

Addition of Entities to the Entity List

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Final rule.

SUMMARY: In this rule, the Bureau of Industry and Security (BIS) amends the Export Administration Regulations (EAR) by adding Huawei Technologies Co., Ltd. (Huawei) to the Entity List. The U.S. Government has determined that there is reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States. BIS is also adding non-U.S. affiliates of Huawei to the Entity List because those affiliates pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States. Huawei will be listed on the Entity List under the destination of China. This final rule also adds to the Entity List sixty-eight non-U.S. affiliates of Huawei located in twenty-six destinations: Belgium, Bolivia, Brazil, Burma, Canada, Chile, China, Egypt, Germany, Hong Kong, Jamaica, Japan, Jordan, Lebanon, Madagascar, Netherlands, Oman, Pakistan, Paraguay, Qatar, Singapore, Sri Lanka, Switzerland, Taiwan, United Kingdom, and Vietnam.

DATES: *Effective Date:* This rule is effective May 16, 2019.

FOR FURTHER INFORMATION CONTACT: Director, Office of Exporter Services, Bureau of Industry and Security, Department of Commerce, Phone: (949) 660–0144 or (408) 998–8806 or email your inquiry to: *ECDOEXS@bis.doc.gov.*

SUPPLEMENTARY INFORMATION:

Background

The Entity List (Supplement No. 4 to part 744) identifies entities reasonably believed to be involved, or pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States. The Export Administration Regulations (EAR) (15 CFR, subchapter C, parts 730–774) imposes additional license requirements on, and limits the availability of most license exceptions for exports, reexports, and transfers (in-country) to, listed entities. The license review policy for each listed entity is identified in the ''License review policy'' column on the Entity List, and the impact on the availability of license exceptions is described in the relevant **Federal Register** notice adding entities to the Entity List. BIS places entities on the Entity List pursuant to part 744 (Control Policy: End-User and End-Use Based) and part 746 (Embargoes and Other Special Controls) of the EAR.

The End-User Review Committee (ERC), composed of representatives of the Departments of Commerce (Chair), State, Defense, Energy and, where appropriate, the Treasury, makes all decisions regarding additions to, removals from, or other modifications to the Entity List. The ERC makes all decisions to add an entry to the Entity List by majority vote and all decisions to remove or modify an entry by unanimous vote.

ERC Entity List Decision

Additions to the Entity List

Under § 744.11(b) (Criteria for revising the Entity List) of the EAR, persons for whom there is reasonable cause to believe, based on specific and articulable facts, that the person has been involved, is involved, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States and those acting on behalf of such persons may be added to the Entity List.

Pursuant to § 744.11(b) of the EAR, the ERC has determined that there is reasonable cause to believe that Huawei Technologies Co., Ltd. (Huawei) has been involved in activities determined to be contrary to the national security or foreign policy interests of the United States. To illustrate, Huawei has been indicted in the U.S. District Court for the Eastern District of New York on 13 counts of violating U.S. law (Superseding Indictment), including violations of the International Emergency Economic Powers Act (IEEPA), by knowingly and willfully causing the export, reexport, sale and supply, directly and indirectly, of goods, technology and services (banking and other financial services) from the United States to Iran and the government of Iran without obtaining a license from the Department of Treasury's Office of Foreign Assets Control (OFAC), as required by OFAC's Iranian Transactions and Sanctions Regulations (31 CFR part 560), and conspiracy to violate IEEPA by knowingly and willfully conspiring to cause the export, reexport, sale and supply, directly and indirectly, of goods, technology and services (banking and other financial services) from the United States to Iran and the government of Iran without obtaining a license from OFAC as required by OFAC's Iranian Transactions and Sanctions Regulations (31 CFR part 560). The Superseding Indictment also alleges that Huawei and an Iranian-based affiliate, working with others, knowingly and willfully conspired to impair, impede, obstruct, and defeat, through deceitful and dishonest means, the lawful government operations of OFAC.

Further, Huawei's affiliates present a significant risk of acting on Huawei's behalf to engage in such activities. Because the ERC has determined that there is reasonable cause to believe that the affiliates pose a significant risk of becoming involved in activities contrary to the national security or foreign policy interests of the United States due to their relationship with Huawei, this final rule also adds to the Entity List sixty-eight non-U.S. affiliates of Huawei located in twenty-six destinations: Belgium, Bolivia, Brazil, Burma, Canada, Chile, China, Egypt, Germany, Hong Kong, Jamaica, Japan, Jordan, Lebanon, Madagascar, Netherlands, Oman, Pakistan, Paraguay, Qatar, Singapore, Sri Lanka, Switzerland,

Taiwan, United Kingdom, and Vietnam. Without the imposition of a license requirement as to these affiliated companies, there is reasonable cause to believe that Huawei would seek to use these entities to evade the restrictions imposed by its addition to the Entity List. As set forth in the Superseding Indictment filed in the Eastern District of New York, Huawei participated along with certain affiliates in the alleged criminal violations of U.S. law, including one or more non-U.S. affiliates. The Superseding Indictment also alleges that Huawei and affiliates acting on Huawei's behalf engaged in a series of deceptive and obstructive acts designed to evade U.S. law and to avoid detection by U.S. law enforcement.

In light of the foregoing, Huawei and sixty-eight non-U.S. affiliates of Huawei raise sufficient concern that prior review of exports, reexports, or transfers (in-country) of items subject to the EAR involving these entities, and the possible imposition of license conditions or license denials on shipments to these entities, will enhance BIS's ability to prevent activities contrary to the national security or foreign policy interests of the United States.

For all of the entities added to the Entity List in this final rule, unless authorized by the *Savings Clause* in this final rule, BIS imposes a license requirement for all items subject to the EAR and a license review policy of presumption of denial. Similarly, no license exceptions are available for exports, reexports, or transfers (in-country) to the persons being added to the Entity List in this rule except as allowed in the *Savings Clause* in this final rule.

This final rule adds the following entity to the Entity List:

China

(1) *Huawei Technologies Co., Ltd. (Huawei),* Bantian Huawei Base, Longgang District, Shenzhen, 518129, China.

This final rule also adds the following sixty-eight non-U.S. affiliates of the entry above to the Entity List:

Belgium

(1) *Huawei Technologies Research & Development Belgium NV,* Belgium.

Bolivia

(1) *Huawei Technologies (Bolivia) S.R.L.,* La Paz, Bolivia.

Brazil

(1) *Huawei do Brasil Telecomunicacões Ltda,* Sao Paulo, Brazil.

Burma

(1) *Huawei Technologies (Yangon) Co., Ltd.,* Yangon, Burma.

Canada

(1) *Huawei Technologies Canada Co., Ltd.,* Markham, ON, Canada.

Chile

(1) *Huawei Chile S.A.,* Santiago, Chile.

China

(1) *Beijing Huawei Digital Technologies Co., Ltd.,* Beijing, China;
(2) *Chengdu Huawei High-Tech Investment Co., Ltd.,* Chengdu, Sichuan, China;
(3) *Chengdu Huawei Technologies Co., Ltd.,* Chengdu, Sichuan, China;
(4) *Dongguan Huawei Service Co., Ltd.,* Dongguan, Guangdong, China;
(5) *Dongguan Lvyuan Industry Investment Co., Ltd.,* Dongguan, Guangdong, China;
(6) *Gui'an New District Huawei Investment Co., Ltd.,* Guiyang, Guizhou, China;
(7) *Hangzhou Huawei Digital Technology Co., Ltd.,* Hangzhou, Zhejiang, China;
(8) *HiSilicon Optoelectronics Co., Ltd.,* Wuhan, Hubei, China;
(9) *HiSilicon Technologies Co., Ltd (HiSilicon),* Bantian Longgang District, Shenzhen, 518129, China.
(10) *HiSilicon Tech (Suzhou) Co., Ltd.,* Suzhou, Jiangsu, China;
(11) *Huawei Device Co., Ltd.,* Dongguan, Guangdong, China;
(12) *Huawei Device (Dongguan) Co., Ltd.,* Dongguan, Guangdong, China;
(13) *Huawei Device (Shenzhen) Co., Ltd.,* Shenzhen, Guangdong, China;
(14) *Huawei Digital Technologies (Suzhou) Co., Ltd.,* Suzhou, Jiangsu, China;
(15) *Huawei Machine Co., Ltd.,* Dongguan, Guangdong, China;
(16) *Huawei Software Technologies Co., Ltd.,* Nanjing, Jiangsu, China;
(17) *Huawei Technical Service Co., Ltd.,* China;
(18) *Huawei Technologies Service Co., Ltd.,* Langfang, Hebei, China;
(19) *Huawei Training (Dongguan) Co., Ltd.,* Dongguan, Guangdong, China;
(20) *Huayi Internet Information Service Co., Ltd.,* Shenzhen, Guangdong, China;
(21) *North Huawei Communication Technology Co., Ltd.,* Beijing, China;
(22) *Shanghai Haisi Technology Co., Ltd.,* Shanghai, China;
(23) *Shanghai Huawei Technologies Co. Ltd.,* Shanghai, China;
(24) *Shanghai Mossel Trade Co., Ltd.,* Shanghai, China;
(25) *Shenzhen Huawei Technical Services Co., Ltd.,* Shenzhen, Guangdong, China;
(26) *Shenzhen Huawei Terminal Commercial Co., Ltd.,* Shenzhen, Guangdong, China;
(27) *Shenzhen Huawei Training School Co., Ltd.,* Shenzhen, Guangdong, China;
(28) *Shenzhen Huayi Loan Small Loan Co., Ltd.,* Shenzhen, Guangdong, China;
(29) *Shenzhen Legrit Technology Co., Ltd.,* Shenzhen, Guangdong, China;
(30) *Shenzhen Smartcom Business Co., Ltd.,* Shenzhen, Guangdong, China;
(31) *Suzhou Huawei Investment Co., Ltd.,* Suzhou, Jiangsu, China;
(32) *Wuhan Huawei Investment Co., Ltd.,* Wuhan, Hubei, China;
(33) *Xi'an Huawei Technologies Co., Ltd.,* Xi'an, Shaanxi, China;
(34) *Xi'an Ruixin Investment Co., Ltd.,* Xi'an, Shaanxi, China; *and*
(35) *Zhejiang Huawei Communications Technology Co., Ltd.,* Hangzhou, Zhejiang, China.

Egypt

(1) *Huawei Technology,* Cairo, Egypt.

Germany

(1) *Huawei Technologies Deutschland GmbH,* Germany.

Hong Kong

(1) *Huawei Device (Hong Kong) Co., Limited,* Tsim Sha Tsui, Kowloon, Hong Kong;
(2) *Huawei International Co., Limited,* Hong Kong;
(3) *Huawei Tech. Investment Co., Limited,* Hong Kong;
(4) *Huawei Technologies Co. Ltd.,* Tsim Sha Tsui, Kowloon, Hong Kong;
(5) *Hua Ying Management Co. Limited,* Tsim Sha Tsui, Kowloon, Hong Kong; *and*
(6) *Smartcom (Hong Kong) Co., Limited,* Sheung Wan, Hong Kong;

Jamaica

(1) *Huawei Technologies Jamaica Company Limited,* Kingston, Jamaica.

Japan

(1) *Huawei Technologies Japan K.K.,* Japan.

Jordan

(1) *Huawei Technologies Investment Co. Ltd.,* Amman, Jordan.

Lebanon

(1) *Huawei Technologies Lebanon,* Beirut, Lebanon.

Madagascar

(1) *Huawei Technologies Madagascar Sarl,* Antananarivo, Madagascar.

Netherlands

(1) *Huawei Technologies Coöperatief U.A.,* Netherlands.

Oman

(1) *Huawei Tech Investment Oman LLC,* Muscat, Oman.

Pakistan

(1) *Huawei Technologies Pakistan (Private) Limited,* Islamabad, Pakistan.

Paraguay

(1) *Huawei Technologies Paraguay S.A.,* Asuncion, Paraguay.

Qatar

(1) *Huawei Tech Investment Limited,* Doha, Qatar.

Singapore

(1) *Huawei International Pte. Ltd.,* Singapore.

Sri Lanka

(1) *Huawei Technologies Lanka Company (Private) Limited,* Colombo, Sri Lanka.

Switzerland

(1) *Huawei Technologies Switzerland AG,* Liebefeld, Bern, Switzerland.

Taiwan

(1) *Xunwei Technologies Co., Ltd.,* Taipei, Taiwan.

United Kingdom

(1) *Huawei Global Finance (UK) Limited,* Great Britain;
(2) *Proven Glory,* British Virgin Islands; *and*
(3) *Proven Honour,* British Virgin Islands.

Vietnam

(1) *Huawei Technologies (Vietnam) Company Limited,* Hanoi, Vietnam; *and*
(2) *Huawei Technology Co. Ltd.,* Hanoi, Vietnam.

Savings Clause

Shipments of items removed from eligibility for a License Exception or export or reexport without a license (NLR) as a result of this regulatory action that were en route aboard a carrier to a port of export or reexport, on May 16, 2019, pursuant to actual orders for export or reexport to a foreign destination, may proceed to that destination under the previous eligibility for a License Exception or export or reexport without a license (NLR).

Export Control Reform Act of 2018

On August 13, 2018, the President signed into law the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which included the Export Control Reform Act of 2018 (ECRA) (Title XVII, Subtitle B of Pub. L. 115–232 (132 Stat. 2210); 50 U.S.C. 4801 *et seq.*), which provides the legal basis for BIS's principal authorities and serves as the authority under which BIS issues this rule. As set forth in sec. 1768 of ECRA, all delegations, rules, regulations, orders, determinations, licenses, or other forms of administrative action that have been made, issued, conducted, or allowed to become effective under the Export Administration Act of 1979 (50 U.S.C. 4601 *et seq.*) (as in effect prior to August 13, 2018 and as continued in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) and Executive Order 13222 of August 17, 2001, 3 CFR, 2001 Comp., p. 783 (2002), as amended by Executive Order 13637 of March 8, 2013, 78 FR 16129 (March 13, 2013), and as extended by the Notice of August 8, 2018, 83 FR 39871 (August 13, 2018)), or the Export Administration Regulations, and are in effect as of August 13, 2018, shall continue in effect according to their terms until modified, superseded, set aside, or revoked under the authority of ECRA.

Rulemaking Requirements

1. Executive Orders 13563 and 12866 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been determined to be not significant for purposes of Executive Order 12866. This rule is not an Executive Order 13771 regulatory action because this rule is not significant under Executive Order 12866.

2. Notwithstanding any other provision of law, no person is required to respond to nor be subject to a penalty for failure to comply with a collection of information, subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA), unless that collection of information displays a currently valid Office of Management and Budget (OMB) Control Number. This regulation involves collections previously approved by OMB under control number 0694–0088, Simplified Network Application Processing System, which includes, among other things, license applications and carries a burden estimate of 42.5 minutes for a manual or electronic submission. Total burden hours associated with the PRA and OMB control number 0694–0088 are not expected to increase as a result of this rule. You may send comments regarding the collection of information associated with this rule, including suggestions for reducing the burden, to Jasmeet K. Seehra, Office of Management and Budget (OMB), by email to *Jasmeet_K._Seehra@omb.eop.gov,* or by fax to (202) 395–7285.

3. This rule does not contain policies with Federalism implications as that term is defined in Executive Order 13132.

4. Pursuant to sec. 1762 of ECRA, this action is exempt from the Administrative Procedure Act (5 U.S.C. 553) requirements for notice of proposed rulemaking, opportunity for public participation, and delay in effective date.

5. Because a notice of proposed rulemaking and an opportunity for public comment are not required to be given for this rule by 5 U.S.C. 553, or by any other law, the analytical requirements of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.,* are not applicable. Accordingly, no regulatory flexibility analysis is required and none has been prepared.

List of Subjects in 15 CFR Part 744

Exports, Reporting and recordkeeping requirements, Terrorism.

Accordingly, part 744 of the Export Administration Regulations (15 CFR parts 730–774) is amended as follows:

PART 744—[AMENDED]

■ 1. The authority citation for 15 CFR part 744 is revised to read as follows:

Authority: Pub. L. 115–232, Title XVII, Subtitle B (132 Stat. 2210); 50 U.S.C. 4801 *et seq.;* 50 U.S.C. 1701 *et seq.;* 22 U.S.C. 3201 *et seq.;* 42 U.S.C. 2139a; 22 U.S.C. 7201 *et seq.;* 22 U.S.C. 7210; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 12947, 60 FR 5079, 3 CFR, 1995 Comp., p. 356; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13099, 63 FR 45167, 3 CFR, 1998 Comp., p. 208; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; E.O. 13224, 66 FR 49079, 3 CFR, 2001 Comp., p. 786; Notice of August 8, 2018, 83 FR 39871 (August 13, 2018); Notice of September 19, 2018, 83 FR 47799 (September 20, 2018). Notice of November 8, 2018, 83 FR 56253 (November 9, 2018); Notice of January 16, 2019, 84 FR 127 (January 18, 2019).

■ 2. Supplement No. 4 to part 744 is amended:

■ a. By adding in alphabetical order a heading for Belgium and one Belgian

entity, ''Huawei Technologies Research & Development Belgium NV''.

■ b. By adding in alphabetical order a heading for Bolivia and one Bolivian entity, ''Huawei Technologies (Bolivia) S.R.L.''.

■ c. By adding in alphabetical order a heading for Brazil and one Brazilian entity, ''Huawei do Brasil Telecomunicacões Ltda''.

■ d. By adding in alphabetical order a heading for Burma and one Burmese entity, ''Huawei Technologies (Yangon) Co., Ltd.''.

■ e. Under Canada, by adding in alphabetical order, one Canadian entity, ''Huawei Technologies Canada Co., Ltd''.

■ f. By adding in alphabetical order a heading for Chile and one Chilean entity, ''Huawei Chile S.A.''.

■ g. Under China, People's Republic of, by adding in alphabetical order, thirty-six Chinese entities: ''Beijing Huawei Digital Technologies Co., Ltd.'', ''Chengdu Huawei High-Tech Investment Co., Ltd.'', ''Chengdu Huawei Technologies Co., Ltd.'', ''Dongguan Huawei Service Co., Ltd.'', ''Dongguan Lvyuan Industry Investment Co., Ltd.'', ''Gui'an New District Huawei Investment Co., Ltd.'', ''Hangzhou Huawei Digital Technology Co., Ltd.'', ''HiSilicon Optoelectronics Co., Ltd.'', ''HiSilicon Technologies Co., Ltd (HiSilicon)'', ''HiSilicon Tech (Suzhou) Co., Ltd.'', ''Huawei Device Co., Ltd.'', ''Huawei Device (Dongguan) Co., Ltd.'', ''Huawei Device (Shenzhen) Co., Ltd.'', ''Huawei Digital Technologies (Suzhou) Co., Ltd.'', ''Huawei Machine Co., Ltd.'', ''Huawei Software Technologies Co., Ltd.'', ''Huawei Technical Service Co., Ltd.'', ''Huawei Technologies Co., Ltd.'', ''Huawei Technologies Service Co., Ltd.'', ''Huawei Training (Dongguan) Co., Ltd.'', ''Huayi internet Information Service Co., Ltd.'', ''North Huawei Communication Technology Co., Ltd.'', ''Shanghai Haisi Technology Co., Ltd.'', ''Shanghai Huawei Technologies Co. Ltd.'', ''Shanghai Mossel Trade Co., Ltd.'', ''Shenzhen Huawei Technical Services Co., Ltd.'', ''Shenzhen Huawei Terminal Commercial Co., Ltd.'', ''Shenzhen Huawei Training School Co., Ltd.'', ''Shenzhen Huayi Loan Small Loan Co., Ltd.'', ''Shenzhen Legrit Technology Co., Ltd.'', ''Shenzhen Smartcom Business Co., Ltd.'', ''Suzhou Huawei Investment Co., Ltd.'', ''Wuhan Huawei Investment Co., Ltd.'', ''Xi'an Huawei Technologies Co., Ltd.'', ''Xi'an Ruixin Investment Co., Ltd.'', and ''Zhejiang Huawei Communications Technology Co., Ltd.''.

■ h. Under Egypt, by adding in alphabetical order, one Egyptian entity, ''Huawei Technology''.

■ i. Under Germany, by adding in alphabetical order, one German entity, ''Huawei Technologies Deutschland GmbH''.

■ j. Under Hong Kong, by adding in alphabetical order, six Hong Kong entities, ''Huawei Device (Hong Kong) Co., Limited'', ''Huawei International Co., Limited'', ''Huawei Tech. Investment Co., Limited'', ''Huawei Technologies Co. Ltd.'', ''Hua Ying Management Co. Limited'', and ''Smartcom (Hong Kong) Co., Limited''.

■ k. By adding in alphabetical order a heading for Jamaica and one Jamaican entity, ''Huawei Technologies Jamaica Company Limited''.

■ l. By adding in alphabetical order a heading for Japan and one Japanese entity, ''Huawei Technologies Japan K.K.''.

■ m. By adding in alphabetical order a heading for Jordan and one Jordanian entity, ''Huawei Technologies Investment Co. Ltd.''.

■ n. By adding in alphabetical order, under Lebanon, one Lebanese entity, ''Huawei Technologies Lebanon''.

■ o. By adding in alphabetical order a heading for Madagascar and one Malagasy entity, ''Huawei Technologies Madagascar Sarl''.

■ p. Under Netherlands, by adding in alphabetical order, one Dutch entity, ''Huawei Technologies Coöperatief U.A.''.

■ q. By adding in alphabetical order a heading for Oman and one Omani entity, ''Huawei Tech Investment Oman LLC''.

■ r. Under Pakistan, by adding in alphabetical order, one Pakistani entity, ''Huawei Technologies Pakistan (Private) Limited''.

■ s. By adding in alphabetical order a heading for Paraguay and one Paraguayan entity, ''Huawei Technologies Paraguay S.A.''.

■ t. By adding in alphabetical order a heading for Qatar and one Qatari entity, ''Huawei Tech Investment Limited''.

■ u. Under Singapore, by adding in alphabetical order, one Singaporean entity, ''Huawei International Pte. Ltd.''.

■ v. By adding in alphabetical order a heading for Sri Lanka and one Sinhalese entity, ''Huawei Technologies Lanka Company (Private) Limited''.

■ w. Under Switzerland, by adding in alphabetical order, one Swiss entity, ''Huawei Technologies Switzerland AG''.

■ x. Under Taiwan, by adding in alphabetical order, one Taiwanese entity, ''Xunwei Technologies Co., Ltd.''

■ y. Under United Kingdom, by adding in alphabetical order, three British entities, ''Huawei Global Finance (UK) Limited'', ''Proven Glory'', and ''Proven Honour''.

■ z. By adding in alphabetical order a heading for Vietnam and two Vietnamese entities, ''Huawei Technologies (Vietnam) Company Limited'' and ''Huawei Technology Co. Ltd.''.

The additions read as follows:

Supplement No. 4 to Part 744—Entity List

* * * * *

Country	Entity	License requirement	License review policy	**Federal Register** citation
*	*	*	*	*
BELGIUM	Huawei Technologies Research & Development Belgium NV, Belgium.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
*	*	*	*	*
BOLIVIA	Huawei Technologies (Bolivia) S.R.L., La Paz, Bolivia.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
BRAZIL	Huawei do Brasil Telecomunicacões Ltda, Sao Paulo, Brazil.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.

Country	Entity	License requirement	License review policy	Federal Register citation
*	* * *	*	* *	*
BURMA	Huawei Technologies (Yangon) Co., Ltd., Yangon, Burma.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
CANADA	* *	* *	*	*
	Huawei Technologies Canada Co., Ltd., Markham, ON, Canada.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
CHILE	Huawei Chile S.A., Santiago, Chile.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
CHINA, PEOPLE'S REPUBLIC OF.	* *	* *	*	*
	Beijing Huawei Digital Technologies Co., Ltd., Beijing, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Chengdu Huawei High-Tech Investment Co., Ltd., Chengdu, Sichuan, China.	For all items subject to the EAR. (See § 744.11 of the EAR),	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Chengdu Huawei Technologies Co., Ltd., Chengdu, Sichuan, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Dongguan Huawei Service Co., Ltd., Dongguan, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Dongguan Lvyuan Industry Investment Co., Ltd., Dongguan, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Gui'an New District Huawei Investment Co., Ltd., Guiyang, Guizhou, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Hangzhou Huawei Digital Technology Co., Ltd., Hangzhou, Zhejiang, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	HiSilicon Optoelectronics Co., Ltd., Wuhan, Hubei, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	HiSilicon Technologies Co., Ltd (HiSilicon), Bantian Longgang District, Shenzhen, 518129, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	HiSilicon Tech (Suzhou) Co., Ltd., Suzhou, Jiangsu, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Device Co., Ltd., Dongguan, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Device (Dongguan) Co., Ltd., Dongguan, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Device (Shenzhen) Co., Ltd., Shenzhen, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Digital Technologies (Suzhou) Co., Ltd., Suzhou, Jiangsu, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Machine Co., Ltd., Dongguan, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Software Technologies Co., Ltd., Nanjing, Jiangsu, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Technologies Co., Ltd., Bantian Huawei Base, Longgang District, Shenzhen, 518129, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Technical Service Co., Ltd., China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Technologies Service Co., Ltd., Langfang, Hebei, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Training (Dongguan) Co., Ltd., Dongguan, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huayi Internet Information Service Co., Ltd., Shenzhen, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.

Country	Entity	License requirement	License review policy	**Federal Register** citation
	* *	* *	*	*
	North Huawei Communication Technology Co., Ltd., Beijing, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Shanghai Haisi Technology Co., Ltd., Shanghai, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Shanghai Huawei Technologies Co. Ltd., Shanghai, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Shanghai Mossel Trade Co., Ltd., Shanghai, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Shenzhen Huawei Technical Services Co., Ltd., Shenzhen, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Shenzhen Huawei Terminal Commercial Co., Ltd., Shenzhen, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Shenzhen Huawei Training School Co., Ltd., Shenzhen, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Shenzhen Huayi Loan Small Loan Co., Ltd., Shenzhen, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Shenzhen Legrit Technology Co., Ltd., Shenzhen, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Shenzhen Smartcom Business Co., Ltd., Shenzhen, Guangdong, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Suzhou Huawei Investment Co., Ltd., Suzhou, Jiangsu, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Wuhan Huawei Investment Co., Ltd., Wuhan, Hubei, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Xi'an Huawei Technologies Co., Ltd., Xi'an, Shaanxi, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Xi'an Ruixin Investment Co., Ltd., Xi'an, Shaanxi, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Zhejiang Huawei Communications Technology Co., Ltd., Hangzhou, Zhejiang, China.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
*	* * *	* *	* *	*
EGYPT	* *	* *	*	*
	Huawei Technology, Cairo, Egypt.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
*	* * *	* *	* *	*
GERMANY	* *	* *	*	*
	Huawei Technologies Deutschland GmbH, Germany.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
*	* * *	* *	* *	*
HONG KONG	* *	* *	*	*
	Huawei Device (Hong Kong) Co., Limited, Tsim Sha Tsui, Kowloon, Hong Kong.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei International Co., Limited, Hong Kong.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.

Country	Entity	License requirement	License review policy	Federal Register citation
	Huawei Tech. Investment Co., Limited, Hong Kong.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Technologies Co. Ltd., Tsim Sha Tsui, Kowloon, Hong Kong.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Hua Ying Management Co. Limited, Tsim Sha Tsui, Kowloon, Hong Kong.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
	Smartcom (Hong Kong) Co., Limited, Sheung Wan, Hong Kong.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
*	* * *	*	* *	*
JAMAICA	Huawei Technologies Jamaica Company Limited, Kingston, Jamaica.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
JAPAN	Huawei Technologies Japan K.K., Japan.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
JORDAN	Huawei Technologies Investment Co. Ltd., Amman, Jordan.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
*	* * *	*	* *	*
LEBANON	* *	* *	*	*
	Huawei Technologies Lebanon, Beirut, Lebanon.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
MADAGASCAR	Huawei Technologies Madagascar Sarl, Antananarivo, Madagascar.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
*	* * *	*	* *	*
NETHERLANDS	* *	* *	*	*
	Huawei Technologies Coöperatief U.A., Netherlands.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
*	* * *	*	* *	*
OMAN	Huawei Tech Investment Oman LLC, Muscat, Oman.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
PAKISTAN	* *	* *	*	*
	Huawei Technologies Pakistan (Private) Limited, Islamabad, Pakistan.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
*	* * *	*	* *	*
PARAGUAY	Huawei Technologies Paraguay S.A., Asuncion, Paraguay.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
*	* * *	*	* *	*
QATAR	Huawei Tech Investment Limited, Doha, Qatar.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
*	* * *	*	* *	*
SINGAPORE	* *	* *	*	*
	Huawei International Pte. Ltd., Singapore.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*

Country	Entity	License requirement	License review policy	**Federal Register** citation
*	* * *	*	* *	*
SRI LANKA	Huawei Technologies Lanka Company (Private) Limited, Colombo, Sri Lanka.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
*	* * *	*	* *	*
SWITZERLAND	* *	* *	*	*
	Huawei Technologies Switzerland AG, Liebefeld, Bern, Switzerland.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
*	* * *	*	* *	*
TAIWAN	* *	* *	*	*
	Xunwei Technologies Co., Ltd., Taipei, Taiwan.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	*
*	* * *	*	* *	*
UNITED KINGDOM	* *	* *	*	*
	Huawei Global Finance (UK) Limited, Great Britain.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	* *
	Proven Glory, British Virgin Islands	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Proven Honour, British Virgin Islands.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	* *	* *	*	* *
VIETNAM	Huawei Technologies (Vietnam) Company Limited, Hanoi, Vietnam.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.
	Huawei Technology Co. Ltd., Hanoi, Vietnam.	For all items subject to the EAR. (See § 744.11 of the EAR).	Presumption of denial	84 FR [INSERT FR PAGE NUMBER] May 21, 2019.

Dated: May 16, 2019.

Wilbur Ross,

Secretary of Commerce.

[FR Doc. 2019–10616 Filed 5–16–19; 4:15 pm]

BILLING CODE 3510–33–P

DEPARTMENT OF STATE

22 CFR Part 41

[Public Notice: 10726]

RIN 1400–AD93

Visa Information Update Requirements Under the Electronic Visa Update System (EVUS)

AGENCY: Department of State.

ACTION: Final rule; confirmation of effective date.

SUMMARY: The Department of State is confirming the effective date of November 29, 2016, for the final rule that published in the **Federal Register** of October 26, 2016, instituting a requirement for nonimmigrant aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category to provide required information to DHS after the receipt of his or her visa of a designated category.

DATES: The effective date of final rule published in the **Federal Register** of October 20, 2016 (81 FR 72522), is confirmed: November 29, 2016.

FOR FURTHER INFORMATION CONTACT: Taylor Beaumont, Acting Division Chief, U.S. Department of State, Office of Legislation and Regulations, CA/VO/L/R, 600 19th Street NW, Washington, DC 20522, (202) 485–8910, *VisaRegs@state.gov*.

SUPPLEMENTARY INFORMATION: The Department published a final rule, Public Notice 9530 at 81 FR 72522, October 20, 2016, with a request for comments, amending sections of part 41 of title 22 of the Code of Federal Regulations. The rule provided modifications to the visa revocation regulations, which, with the the DHS rule amending 8 CFR part 215, subpart B (RIN 1651–AB08), created the Electronic Visa Update System (EVUS). As provided in 8 CFR part 215, subpart B, EVUS is an online information update system that requires nonimmigrant aliens who hold a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category to enroll in EVUS by providing information to DHS after the receipt their visa. The final rule became effective on November 29, 2016, and remains unchanged.

Analysis of Comments: The final rule was published with request for comments on October 20, 2016, Vol. 81, No. 203, Page 72522. The comment period closed on December 19, 2016. The Department received one non-responsive comment to the final rule. As the comment was non-responsive, it does not provide a basis to reconsider the rule.

Chapter 30

US Department of Commerce Adds 46 Huawei Affiliates to Entity List (Brian Heater)

US Commerce Department adds 46 Huawei affiliates to entity list

Brian Heater@bheater / • August 19, 2019

Source: https://techcrunch.com/2019/08/19/us-commerce-department-adds-46-huawei-affiliates-to-entity-list/

Image Credits: Jaap Arriens/NurPhoto / Getty Images

Update: Huawei has responded to the DoC's move,

> We oppose the US Commerce Department's decision to add another 46 Huawei affiliates to the Entity List. It's clear that this decision, made at this particular time, is politically motivated and has nothing to do with national security. These actions violate the basic principles of free market competition. They are in no one's interests, including US companies. Attempts to suppress Huawei's business won't help the United States achieve technological leadership. We call on the US government to put an end to this unjust treatment and remove Huawei from the Entity List.

The United States Department of Commerce announced this morning the addition of 46 Huawei affiliates to its Entity List. Effective today, the companies join more than 100 entries added to the list over connections to the embattled Chinese consumer electronics giant.

The DoC also used this morning's news to announce an extension of its Temporary General License (TGL), which affords people and companies a limited time use of goods from Huawei and affiliate companies in order to essentially wean them off of Huawei networking equipment. The license, which offers "narrow exceptions" is set to expire 90 days from today.

In a statement provided to the press, Secretary of Commerce Wilbur Ross stated, "As we continue to urge consumers to transition away from Huawei's products, we recognize that more time is necessary to prevent any disruption. Simultaneously, we are constantly working at the Department to ensure that any exports to Huawei and its affiliates do not violate the terms of the Entity Listing or Temporary General License."

Huawei has, of course, long denied any ties to security or spying accusations from the U.S. government. Recently, stories, including alleged ties to African government spying, have continued to shine a light on concerns about the company's ties to the Chinese government. Those concerns have led to Huawei's addition to the entities list, along with U.S. government bans on buying equipment.

Per the DoC:

> Huawei was added to the Entity List after the Department concluded that the company is engaged in activities that are contrary to U.S. national security or foreign policy interests, including alleged violations of the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA by providing prohibited financial services to Iran, and obstruction of justice in connection with the investigation of those alleged violations of U.S. sanctions, among other illicit activities.

Losing access to American software and hardware could, in turn, have a devastating impact on the company. Notably, Huawei recently unveiled HarmonyOS. The new mobile operating system is not yet an Android replacement, but is believed by many to be part of a long-term strategy to wean itself off of dependence on Google.

We have reached out to Huawei for comment.

Chapter 31

Linux Foundation Statement on Huawei Entity List Ruling

Linux Foundation Statement on Huawei Entity List Ruling

By The Linux Foundation | May 23, 2019

We have received inquiries regarding concerns about a member subject to an Entity List Ruling. [1] The Huawei Entity List ruling was specifically scoped to activities and transactions subject to the Export Administration Regulations (EAR).

Open Source Software Not involving Encryption

The Linux Foundation is a free and open source software organization whose project communities publish collaboratively developed software publicly. All software published by Linux Foundation projects is made available to the public without restrictions other than those imposed by the open source licenses. Software that is published publicly, such as open source software, is not subject to the EAR [2], and therefore not relevant to the Entity List Ruling.

Open Source Encryption Software

Open source encryption software source code was reclassified by the US Department of Commerce, Bureau of Industry and Security (BIS) effective September 20, 2016 as publicly available and no longer subject to the EAR. [3] Each open source project that uses or implements encryption is still required to send a notice of the URL to BIS and NSA to satisfy the publicly available notice requirement in the EAR at 15 CFR § 742.15(b).

The Linux Foundation continues to work with our projects to ensure their notices

participating in training and providing membership or sponsorship funds are all activities which are not subject to the EAR and therefore should have no impact on our communities. If there is a unique situation of concern, we encourage you to reach out directly to legal@linuxfoundation.org.

Security Vulnerability Pre-Disclosure Lists

A few of the Linux Foundation's project communities use security vulnerability pre-disclosure lists to alert known implementers of the project's open source software about vulnerability fixes that will be disclosed by the developers and published publicly in the near future (typically within 2 weeks). In these situations, LF project communities are conveying knowledge, information and written software patches that will be made publicly available when accepted for publication by the committers on the project and such disclosures are permitted under 15 CFR § 734.7(a)(5). [2]

[1] https://www.bis.doc.gov/index.php/documents/regulations-docs/2394-huawei-and-affiliates-entity-list-rule/file

[2] https://www.ecfr.gov/cgi-bin/text-idx?SID=fcba36d2f267c2fdecc5694c1e754aa7&mc=true&node=se15.2.734_17&rgn=div8

[3] 81 Fed. Reg. 64656, 64668 (September 20, 2016). See also, https://www.bis.doc.gov/index.php/policy-guidance/encryption/223-new-encryption

[4] https://www.linuxfoundation.org/export/

Chapter 32

Apache Foundation Statement on Huawei Entity List Ruling

The Apache Software Foundation
Blogging in Action.

The Apache Software Foundation Blog

« The Apache Software... | Main | The Apache News... »

WEDNESDAY MAY 22, 2019

Statement by The Apache Software Foundation regarding US Federal Register Notice of non-US affiliates added to Entity List Ruling

Restrictions on exports and reexports to parties named on Entity List specifically apply to activities and transactions subject to the Export Administration Regulation (EAR). [1] Open Source publicly available encryption software source code, as reclassified by the US Department of Commerce, Bureau of Industry and Security (BIS) effective September 20, 2016, is "publicly available" and "published" and is not "subject to the EAR." [2]

Open Source projects involving encryption software source code are still required to send a notice of the URL to BIS and NSA to satisfy the "publicly available" notice requirement in EAR § 742.15(b).

The ASF continues to work with Apache projects and their communities to ensure their notices are up to date and are maintained in the future.[3]

Open Source software, collaboration on Open Source code, attending open telephonic or in person meetings, and providing sponsorship funds are all activities that are not subject to the EAR and therefore should have no impact on our communities.

For more information, visit http://apache.org/foundation/license-faq.html

Calendar

« October 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Today

Search

Search

Hot Blogs (today's hits)

Tag Cloud

apache apachecon asf at big bigdata cloud community data foundation hadoop initiatives just news open opensource processes project projects round-

Roman Shaposhnik
ASF Vice President Legal Affairs

We thank DLA Piper and The Linux Foundation for their legal counsel and collaboration regarding this subject.

[1] https://www.bis.doc.gov/index.php/documents/regulations-docs/2395-effective-date-of-huawei-and-affiliates-entity-list-rule

[2] 81 Fed. Reg. 64656, 64668 (September 20, 2016). See also, https://www.bis.doc.gov/index.php/policy-guidance/encryption/223-new-encryption

[3] https://www.apache.org/licenses/exports/

Posted at 09:59PM May 22, 2019 by Sally in General | |

Comments:

Post a Comment:

Comments are closed for this entry.

up software
source success
summary the tlp top-level **weekly** why works

Categories

All
General
ApacheCon
Projects
Milestones
SuccessAtApache
Newsletter

Feeds

All
General
ApacheCon
Projects
Milestones
SuccessAtApache
Newsletter
Comments

Links

Planet Apache

Navigation

ASF Blogs
Weblog
Login

Part VI

FOSS and Platforms

Chapter 33

The Separation of Platforms and Commerce (Lina M. Khan)

THE SEPARATION OF PLATFORMS AND COMMERCE

*Lina M. Khan**

A handful of digital platforms mediate a growing share of online commerce and communications. By structuring access to markets, these firms function as gatekeepers for billions of dollars in economic activity. One feature dominant digital platforms share is that they have integrated across business lines such that they both operate a platform and market their own goods and services on it. This structure places dominant platforms in direct competition with some of the businesses that depend on them, creating a conflict of interest that platforms can exploit to further entrench their dominance, thwart competition, and stifle innovation.

This Article argues that the potential hazards of integration by dominant tech platforms invite recovering structural separations. Structural separations have been a mainstay element of American economic regulation. Traditionally applied to critical networks and essential infrastructure, structural separations prohibited entry in certain markets and prevented dominant intermediaries from directly competing with the businesses reliant on their services. In recent decades, structural separations have been largely abandoned. At the same time that lawmakers have weakened or eliminated sector-specific regulatory regimes, judicial interpretation of antitrust law has drastically narrowed the forms of vertical conduct and structures that register as anticompetitive. And when antitrust enforcers have targeted these forms of conduct and structures, they have applied remedies that generally (1) fail to target the underlying source of the problem and (2) overwhelm the institutional capacities of the actors assigned to oversee them. Neglecting structural remedies results in

* Academic Fellow, Columbia Law School. For generous conversations and insightful feedback, I am deeply grateful to Shah Ali, Rebecca Haw Allensworth, David Balan, Commissioner Rohit Chopra, Joshua Fischman, Jeffrey Gordon, David Grewal, Michael Guttentag, Scott Hemphill, Robert Hockett, Jen Howard, Sally Hubbard, Ted Janger, Richard John, Kathryn Judge, Amy Kapczynski, Al Klevorick, William Kovacic, Mark Lemley, Christopher Leonard, Christopher Leslie, Zachary Liscow, Barry Lynn, Jonathan Macey, Daniel Markovits, Doug Melamed, Urja Mittal, Stacy Mitchell, John Morley, Thomas Nachbar, Saule Omarova, Matt Panhans, Frank Pasquale, David Pozen, George Priest, Sabeel Rahman, Blake Reid, Daria Roithmayr, Hal Singer, Ganesh Sitaraman, Dina Srinivasan, Marshall Steinbaum, Matt Stoller, Maurice Stucke, Olivier Sylvain, Zephyr Teachout, Sandeep Vaheesan, Barbara van Schewick, and Tim Wu, as well as participants in Vanderbilt Law School's "The New Infrastructure" roundtable, the Competition, Antitrust Law and Innovation Forum at UC–Irvine, and workshops at Boston College, Brooklyn, Cardozo, Columbia, Cornell, Loyola L.A., University of Michigan, Stanford, Texas A&M, UCLA, University of Southern California–Gould, University of Virginia, and Yale law schools. Many thanks to Jeremy Patashnik and the *Columbia Law Review* for exceptional editorial support.

both substantive harms and institutional misalignments—effects that are especially pronounced in digital platform markets.

This Article seeks to give structural separations a seat back at the table. Tracing the history of separations reveals that they have been motivated by a host of functional goals, ranging from fair competition and system resiliency to media diversity and administrability. Recalling this broader set of concerns brings into focus the range of factors at stake when dealing with dominant intermediaries and invites consideration of the degree to which separations in platform markets would also respond to a diverse set of problems.

INTRODUCTION

> *"No competition can exist between two producers of a commodity when one of them has the power to prescribe both the price and output of the other."*
>
> —U.S. House of Representatives, Committee on Interstate & Foreign Commerce[1]

> *"In short, the choice is between a Bell System restrained by neither regulation nor true competition and a Bell System reorganized in such a way as to diminish greatly the possibility of future anticompetitive behavior."*
>
> —U.S. District Court for the District of Columbia[2]

A handful of digital platforms exert increasing control over key arteries of American commerce and communications. Structuring access to markets, these firms function as gatekeepers for billions of dollars in economic activity. By virtue of setting marketplace rules for the millions of merchants, producers, and developers dependent on their infrastructure, dominant platforms today "function as regulators."[3]

As these platforms further concentrate market power, there are rising concerns about their size—usually in reference to the large share that each firm captures of its primary markets.[4] Yet an equally important question concerns

---

1. H.R. Rep. No. 52-2278, at vii–viii (1893).

2. United States v. AT&T Co., 552 F. Supp. 131, 170 (D.D.C. 1982).

3. See Jacques Crémer et al., European Comm'n, Competition Policy for the Digital Era 6 (2019), http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf [https://perma.cc/LHH7-9UEK].

4. See, e.g., Franklin Foer, World Without Mind: The Existential Threat of Big Tech 103 (2017) ("Amazon doesn't necessarily want to own whole industries, but it likes to control them. With publishing, Amazon has become the indispensable store. It sells 65 percent of all e-books and over 40 percent of all books."); Jonathan Taplin, Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy 21 (2017) ("Google has an 88 percent market share in online searches and search advertising. Google's Android mobile operating system has an 80 percent global market share in its category. Amazon has a 70 percent market share in ebook sales. Facebook has a 77 percent market share in mobile social media."); David Dayen, Big Tech: The New Predatory Capitalism, Am. Prospect (Dec. 26, 2017), http://prospect.org/article/
big-tech-new-predatory-capitalism [https://perma.cc/H2AA-JEXD] (arguing that tech firms, due to their market-share dominance, have "crippled entrepreneurship," "concentrated economic gains in a few small enclaves," "religiously avoid[ed] taxes," developed extensive surveillance capabilities, and created addictive products that "have undermined social relationships, expanded divisiveness, and transformed what it means to be human"); Ben Smith, Opinion, There's Blood in the Water in Silicon Valley, BuzzFeed News (Sept. 12, 2017), https://www.buzzfeednews.com/article/bensmith/theres-blood-in-the-water-in-silicon-valley
[https://perma.cc/3FQA-B3TC] (describing an increasingly prevalent critique of the major American tech firms—Facebook, Amazon, Google, and Apple—as "sinister new centers of unaccountable power").

not the scale of these companies but their structure. One feature dominant digital platforms share is that they have integrated across business lines such that they both operate a platform and market their own goods and services on it. This structure places dominant platforms in direct competition with some of the businesses that depend on them, creating a conflict of interest that platforms can exploit to further entrench their dominance, thwart competition, and stifle innovation.[5]

Consider Spotify's effort to reach users through Apple's iPhone while Apple sought to promote Apple Music. In 2016, Spotify revealed that Apple had blocked the streaming application from the App Store, "continu[ing] a troubling pattern of behavior by Apple to exclude and diminish the competitiveness of Spotify on iOS and as a rival to Apple Music."[6] Or take the challenge faced by Yelp, Foundem, and scores of online services to reach internet users while Google sought to build out its own competitor offerings.[7] In Europe and India, competition authorities have found that Google ranks its own services higher than those offered by rivals, a "search bias" that means anyone competing with Google properties may effectively disappear from Google search results.[8] Merchants that rely on Amazon to reach consumers are in a similar bind: Not only must they jostle for placement against Amazon's own goods, but they also face the constant risk that Amazon will spot their bestselling items and produce them itself.[9] Facebook, equipped with

---

5. See infra sections I.A–.D.

6. Peter Kafka, Spotify Says Apple Won't Approve a New Version of Its App Because It Doesn't Want Competition for Apple Music, Recode (June 30, 2016), https://www.recode.net/2016/6/30/12067578/spotify-apple-app-store-rejection [https://perma.cc/T4XF-JCEJ] (quoting Horacio Gutierrez, General Counsel, Spotify).

7. See Charles Duhigg, The Case Against Google, N.Y. Times (Feb. 20, 2018), https://www.nytimes.com/2018/02/20/magazine/the-case-against-google.html (on file with the *Columbia Law Review*).

8. Findings of search bias prompted antitrust authorities in Europe and India to fine Google for violating competition laws. Natasha Lomas, Google Fined $2.7BN for EU Antitrust Violations over Shopping Searches, TechCrunch (June 27, 2017), https://techcrunch.com/2017/06/27/google-fined-e2-42bn-for-eu-antitrust-violations-over-shopping-searches/ [https://perma.cc/5J57-2KNW]; Natasha Lomas, Google Fined $21.1M for Search Bias in India, TechCrunch (Feb. 9, 2018), https://techcrunch.com/2018/02/09/google-fined-21-1m-for-search-bias-in-india/ [https://perma.cc/RU8L-FZML].

9. See Greg Bensinger, Competing with Amazon on Amazon, Wall St. J. (June 27, 2012), https://www.wsj.com/articles/SB10001424052702304441404577482902055882264 (on file with the *Columbia Law Review*) ("According to some small retailers, the Seattle-based giant appears to be increasingly using its Marketplace—where third-party retailers sell their wares on the Amazon.com site—as a vast laboratory to spot new products to sell, test sales of potential new goods, and exert more control over pricing."); Julie Creswell, How Amazon Steers Shoppers to Its Own Products, N.Y. Times (June 23, 2018), https://www.nytimes.com/2018/06/23/business/amazon-the-brand-buster.html (on file with the *Columbia Law Review*); Robinson Meyer, When Does Amazon Become a Monopoly?, Atlantic (June 16, 2017), https://www.theatlantic.com/technology/archive/2017/06/when-exactly-does-amazon-become-a-monopoly/530616/ [https://perma.cc/3T2B-7DC8] ("[Amazon] is, in short, an Everything Store: not only selling goods but also producing them, not only distributing media from its servers but also renting them out to others."); Eugene Kim,

technology that lets it detect which rival apps are succeeding, would often give companies a choice: Be acquired by Facebook, or watch it roll out a direct replica.[10] Competing with one of these giants on the giant's own turf is rife with hazards.

Venture capitalists now factor this risk into their investment decisions.[11] Indeed, the power of these gatekeeper platforms to steer the fate of countless other firms is described by entrepreneurs and investors as "having a profound impact on innovation in Silicon Valley"[12] and "choking off the start-up world."[13] Venture capitalists now discuss a "kill-zone" around digital giants—"areas not worth operating or investing in, since defeat is guaranteed."[14] Discussing how

---

Amazon Is Doubling Down on Its Private Label Business, Stoking 'Huge Fear' in Some Sellers, CNBC (Oct. 6, 2018), https://www.cnbc.com/2018/10/06/amazon-doubling-down-on-private-label-sellers-see-huge-fear.html [https://perma.cc/NZC8-XEVA] [hereinafter Kim, Amazon Is Doubling Down].

10. See Elizabeth Dwoskin, Facebook's Willingness to Copy Rivals' Apps Seen as Hurting Innovation, Wash. Post (Aug. 10, 2017), https://www.washingtonpost.com/business/economy/facebooks-willingness-to-copy-rivals-apps-seen-as-hurting-innovation/2017/08/10/ea7188ea-7df6-11e7-a669-b400c5c7e1cc_story.html (on file with the *Columbia Law Review*) (describing Facebook's "aggressive strategy" for attempting to break into fields beyond social networking by "mimic[king] the most successful features of rival companies' apps"); Betsy Morris & Deepa Seetharaman, The New Copycats: How Facebook Squashes Competition from Startups, Wall St. J. (Aug. 9, 2017), https://www.wsj.com/articles/the-new-copycats-how-facebook-squashes-competition-from-startups-1502293444 (on file with the *Columbia Law Review*) [hereinafter Morris & Seetharaman, New Copycats]; Deepa Seetharaman & Betsy Morris, Facebook's Onavo Gives Social-Media Firm Inside Peek at Rivals' Users, Wall St. J. (Aug. 13, 2017), https://www.wsj.com/articles/facebooks-onavo-gives-social-media-firm-inside-peek-at-rivals-users-1502622003 (on file with the *Columbia Law Review*). Faced with criticism that it was using Onavo in potentially anticompetitive ways, Facebook announced in 2019 that it was no longer using the technology to collect data on rivals. See Josh Constine, Facebook Will Shut Down Its Spyware VPN App Onavo, TechCrunch (Feb. 21, 2019), https://techcrunch.com/2019/02/21/facebook-removes-onavo/ [https://perma.cc/5UMD-E5E4].

11. See Dwoskin, supra note 10 ("At Sequoia's annual off-site retreat, held in March, skirting Google and Facebook were main topics of conversation, said Sequoia partner Alfred Lin. . . . 'We don't touch anything that comes too close to Facebook, Google or Amazon,' he said."); Olivia Solon, As Tech Companies Get Richer, Is It 'Game Over' for Startups?, Guardian (Oct. 20, 2017), https://www.theguardian.com/technology/2017/oct/20/tech-startups-facebook-amazon-google-apple [https://perma.cc/BT2G-34G4] ("'People are not getting funded because Amazon might one day compete with them,' said one founder, who wished to remain anonymous. 'If it was startup versus startup, it would have been a fair fight, but startup versus Amazon and it's game over.'"); Asher Schechter, Google and Facebook's "Kill Zone": "We've Taken the Focus Off of Rewarding Genius and Innovation to Rewarding Capital and Scale," ProMarket (May 25, 2018), https://promarket.org/google-facebooks-kill-zone-weve-taken-focus-off-rewarding-genius-innovation-rewarding-capital-scale/ [https://perma.cc/TZ98-LBX6] ("The scale of these companies and their impact on what can be funded, and what can succeed, is massive." (internal quotation marks omitted) (quoting Albert Wenger, Managing Partner, Union Square Ventures)).

12. Dwoskin, supra note 10.

13. Id. (internal quotation marks omitted) (quoting Roger McNamee, Founder, Elevation Partners).

14. Schechter, supra note 11; see also American Tech Giants Are Making Life Tough for Startups, Economist (June 2, 2018), https://www.economist.com/business/2018/06/

tech platform giants today use their integrated structure to undermine rivals, a product manager who worked for Microsoft leading up to its antitrust suit observed, "It's what we did at Microsoft."[15]

Indeed, the way in which dominant online platforms threaten to undermine competition and distort markets today is not entirely new. At its core, the problem traces to a basic challenge posed by firms that capture control over a critical network or channel of distribution. Regulators and competition authorities have traditionally harnessed a set of tools to ensure that bottleneck facilities do not distort competition. These tools include common carriage, which requires firms to offer customers equal access on equal terms,[16] as well as interoperability, which requires networks to maintain an open interface,

---

02/american-tech-giants-are-making-life-tough-for-startups [https://perma.cc/J56F-PML6] (describing venture capitalists' hesitance to support startups in industries dominated by tech giants such as Google, Amazon, and Facebook).

15. Dwoskin, supra note 10 (internal quotation marks omitted) (quoting Scott Sandell, Managing Partner, New Enterprise Associates).

16. See Eli M Noam, Beyond Liberalization II: The Impending Doom of Common Carriage, 18 Telecomm. Pol'y 435, 436–38 (1994) (explaining the origins of common carriage and the underlying principle that no customer willing and able to pay for a service should be denied its use). Recognizing the gatekeeper power of internet service providers (ISPs), academics and policymakers in the 2000s re-embraced common carriage in the form of "network neutrality." Under the Obama Administration, the Federal Communications Commission (FCC) codified net neutrality rules requiring that ISPs treat all internet traffic equally. See Protecting and Promoting the Open Internet, 30 FCC Rcd. 5601, 5603, para. 4 (2015) (adopting "carefully-tailored rules that would prevent specific practices we know are harmful to Internet openness—blocking, throttling, and paid prioritization—as well as a strong standard of conduct designed to prevent the deployment of new practices that would harm Internet openness"); Preserving the Open Internet, Broadband Industry Practices, 25 FCC Rcd. 17905, 17906, para. 1 (2010) (ordering that "[f]ixed broadband providers may not unreasonably discriminate in transmitting lawful network traffic"). In December 2017, the Trump Administration's FCC voted to undo this order. See Restoring Internet Freedom, 33 FCC Rcd. 311, 318, para. 20 (2018). Numerous lawsuits—including one on behalf of twenty-three state attorneys general—are now challenging the legitimacy of the FCC's repeal. See, e.g., Petition for Review at 1–2, New York v. FCC, No. 18-1055 (D.C. Cir. Feb. 22, 2018). A wealth of scholarship has discussed and debated the revival of common carriage in the form of network neutrality. See, e.g., Mark Lemley & Lawrence Lessig, The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era, 48 UCLA L. Rev. 925, 928–30 (2001) (advocating against government policies that reduce competition among internet service providers); Barbara van Schewick, Toward an Economic Framework for Network Neutrality Regulation, 5 J. on Telecomm. & High Tech. L. 329, 331–36 (2007) (analyzing the "potential for discriminatory behavior by network providers"); Kevin Werbach, Only Connect, 22 Berkeley Tech. L.J. 1233, 1270–72 (2007) (noting that, while network neutrality "followed a classic non-discrimination script" when it was first promoted, both sides of the contemporary network neutrality debate "fail to recognize the significance of interconnection"); Tim Wu, Network Neutrality, Broadband Discrimination, 2 J. on Telecomm. & High Tech. L. 141, 150 (2003) [hereinafter Wu, Network Neutrality] (explaining "how a common carriage or anti-discrimination model might be better developed to address the current Internet environment"); Christopher S. Yoo, Beyond Network Neutrality, 19 Harv. J.L. & Tech. 1, 13–18 (2005) (arguing that proponents of network neutrality mistakenly focus on promoting competition among internet content providers, which are already competing vigorously, instead of among internet service providers, which are not currently very competitive).

enabling users to switch between platforms with ease.[17] These policies respond, respectively, to problems of discrimination and lock-in.

In digital markets, however, third parties that depend on a platform risk not just discrimination and lock-in but also appropriation. Because dominant platforms monitor with unrivaled precision the business activity of third parties while also competing with them, a platform can harvest insights gleaned from a producer at the producer's expense.

This Article argues that these combined problems of discrimination and information appropriation invite recovering common carriage's forgotten cousin: structural separations. Structural separations place clear limits on the lines of business in which a firm can engage. Rather than prohibit particular business practices, separations proscribe certain organizational structures. In antitrust, structural remedies are contrasted with behavioral ones: Whereas behavioral remedies seek to prevent firms from engaging in specific types of conduct, structural remedies seek to eliminate the incentives that would make that conduct possible or likely in the first place.[18]

Structural prohibitions have been a traditional element of American economic regulation. They have been applied as a standard regulatory tool and key antitrust remedy in network industries, often to prohibit a dominant intermediary from competing with the businesses that depend on it to get to market. While common carriage regimes prevent a firm from discriminating—requiring equal service on equal terms—structural prohibitions eliminate one source of the incentive to discriminate. In this way, common carriage and structural separations often functioned as complements in the service of nondiscrimination.

Today, structural separations have largely been abandoned.[19] At the same time that lawmakers have significantly weakened or outright eliminated sector-specific regulatory regimes, judicial interpretation of antitrust law has drastically narrowed the forms of vertical conduct and structures that register as anticompetitive. And when antitrust enforcers *have* targeted these forms of conduct and structures in recent years, they've applied remedies that generally (1) fail to target the underlying source of the problem and (2) overwhelm the

17. See Philip J. Weiser, Regulating Interoperability: Lessons from *AT&T*, *Microsoft*, and Beyond, 76 Antitrust L.J. 271, 272–74 (2009) (using the AT&T and Microsoft cases to illuminate why interoperability in an important antitrust tool, and noting that "in network industries, cooperation is essential for rivals of dominant firms to have any chance of success in the marketplace").

18. See Howard A. Shelanski & J. Gregory Sidak, Antitrust Divestiture in Network Industries, 68 U. Chi. L. Rev. 1, 15 (2001) (discussing the distinction between behavioral and structural remedies). It's worth noting that the structural–behavioral divide is not so clear-cut. See Eric Emch et al., What Past U.S. Agency Actions Say About Complexity in Merger Remedies, with an Application to Generic Drug Divestitures 1 (Dusseldorf Inst. for Competition Econ., DICE Discussion Paper No. 270, 2017), https://www.econstor.eu/bitstream/10419/169412/1/898962412.pdf (on file with the *Columbia Law Review*) ("[T]he simple dichotomy of structural versus behavioral does not illuminate the greyer area into which most remedies containing both structural and behavioral elements, fall.").

19. See infra Part II.

institutional capacities of the government actors assigned to oversee them.[20] Neglecting structural separations results in both substantive harms and institutional misalignments—effects that are especially pronounced in digital markets.

This Article seeks to give structural separations a seat back at the table. Its contribution is twofold. First, it demonstrates that both the risk and cost of information appropriation are heightened in digital markets, rendering conduct remedies especially ineffective and structural remedies critical.[21] Dominant digital platforms passively capture highly precise and nuanced data on their business customers, information that they can exploit when competing against those same customers. These data are more valuable by virtue of being more sophisticated—and more likely to be exploited given their value. This risk of appropriation coupled with discrimination, moreover, is especially harmful in digital platform markets, given the important role platforms play as innovation catalysts. Even within a framework where only welfare-based harms justify regulatory interventions, the likely innovation harms stemming from platform appropriation and discrimination invite serious consideration of structural limits.

Second, this Article identifies the host of functional goals that motivated previous separations regimes, ranging from fair competition and system resiliency to media diversity and administrability.[22] These concerns register in a normatively pluralistic framework: While some are cognizable in terms of welfare economics, others appeal to a broader set of democratic and institutionalist values. In the context of business and market structure, these distinct values sometimes align—such that a separation that promotes a robust marketplace of ideas also promotes dynamic efficiency—while in other instances they are in tension.

After identifying the tradition of structural separations and the diverse set of concerns that motivated them,[23] this Article explores whether integration by dominant tech platforms poses risks and challenges analogous to those previously addressed through separations.[24] It closes by briefly sketching out relevant considerations for separating platforms and commerce and identifying likely challenges.[25]

---

20. See Spencer Weber Waller, Access and Information Remedies in High-Tech Antitrust, 8 J. Comp. L. & Econ. 575, 575–77 (2012) ("Finally, the more complex the remedy, the greater the need for sophisticated oversight and dispute resolution mechanisms that typically exceed the resources and strengths of the enforcement agencies.").

21. See infra Part I.

22. See infra Part II.

23. See infra Parts III–IV.

24. See infra Part V.

25. See infra Part V. Although the question of how antitrust enforcers should assess vertical mergers is receiving renewed attention today, the focus of this Article is much narrower: namely, vertical expansion by digital platforms operating in markets characterized by network externalities. Because these markets can favor the emergence of a single dominant player, integration is more likely to raise concerns in network markets than in highly competitive ones. See, e.g., FTC, Commission File No. 181-0180, Statement of Commissioner Rebecca Kelly

This Article is a project in diagnosis and intellectual recovery. It seeks to provide a general analytical framework for thinking through problems stemming from integration by dominant digital platforms and to identify principles through which Congress and agencies can issue policy prescriptions to remedy them. Its goal is to enrich our understanding of the tools and remedies through which lawmakers and regulators have previously addressed integration by dominant intermediaries—an effort in recovery necessitated by the abandonment of traditional regulatory interventions and partial collapse of antitrust. Several questions that this Article only partially engages—such as how to scope and design specific separations in digital markets—invite deeper study.

Several factors render this project especially timely. First, the central role dominant platforms play in structuring access to online commerce and communications is prompting both scholarly and policy discussions about whether these firms should be designated as forms of infrastructure or essential services, meriting regulatory interventions coupled with reinvigorated antitrust.[26] Second, after years of retreating from structural remedies in favor of behavioral ones, antitrust enforcers are confronting the difficulty of enforcing pure conduct remedies and asking whether greater reliance on structural interventions would better promote competition.[27] And third, a neo-Brandeisian movement is refocusing attention on the structural underpinnings of the competitive process, critiquing the current welfare-based approach for both betraying the founding values of antitrust and failing on its own terms.[28]

Slaughter: In the Matter of Sycamore Partners, Staples, and Essendant 2 (2019), https://www.ftc.gov/system/files/documents/public_statements/1448321/181_0180_staples_essendant_slaughter_statement.pdf [https://perma.cc/98Y4-V5EA] ("Vertical tie-ups are occurring across the economy, and they present an enforcement challenge that we must meet.").

26. See, e.g, Ariel Ezrachi & Maurice E. Stucke, Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy 203 (2016) (noting that, while online markets create a "competitive veneer," "complex webs of algorithms" give tech firms new anticompetitive strategies to "maximize the firms' profits, while harming our welfare"); Maurice E. Stucke & Allen P. Grunes, Big Data and Competition Policy 215–16 (2016) (arguing that antitrust authorities should account for "data-driven network effects," which can "increase entry barriers"); K. Sabeel Rahman, The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept, 39 Cardozo L. Rev. 1621, 1626 (2018) [hereinafter Rahman, New Utilities] (identifying "principles for twenty-first century public utility regulation" and applying those principles "to the emergent debates over private power and infrastructure in the context of internet platforms").

27. See Makan Delrahim, Assistant Att'y Gen., Antitrust Div., Dep't of Justice, Keynote Address at American Bar Association's Antitrust Fall Forum (Nov. 16, 2017), https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-keynote-address-american-bar [https://perma.cc/X4H3-Q6KA]; see also John E. Kwoka & Diana L. Moss, Behavioral Merger Remedies: Evaluation and Implications for Antitrust Enforcement, 57 Antitrust Bull. 979, 1008 (2012) ("Structural remedies have advantages in terms of clarity, cost, and certainty, and have withstood the test of experience.").

28. See, e.g., K. Sabeel Rahman, Democracy Against Domination 2–3 (2017) ("Corporations, economic elites, and even market forces themselves all exercise a kind of unchecked power over others in the economy. The purpose of governance in this view is to curtail

Part I of this Article documents how dominant digital platforms use their integrated structure to engage in both discrimination and information appropriation and reviews why this conduct likely undermines innovation. Part II traces the institutional and doctrinal shifts that account for the retreat from structural separations. Part III reviews five instances in which separations were implemented. Part IV identifies the set of harms that lawmakers, regulators, and enforcers sought to address through structural separations and the functional goals they aspired to promote. Part V examines whether integration by dominant platforms gives rise to analogous harms, briefly explores what a separations framework for digital intermediaries might look like, and identifies likely challenges and questions that remain unresolved. The Appendix engages the relevant economic literature to examine why platforms would act in ways that risk undermining their ecosystems.

I. INTEGRATION BY DOMINANT DIGITAL PLATFORMS

Dominant digital platforms serve as critical intermediaries of online commerce and communications. Reflecting on the vital role these firms now play, the Supreme Court has described Facebook, Google, and other online providers as serving as the "modern public square,"[29] while lawmakers have analogized Amazon to a nineteenth-century railroad.[30] Governments around the world have initiated studies and investigations examining the market power these firms enjoy.[31] The dominant digital platforms differ in important ways: They

---

such forms of economic power, subjecting these seemingly powerful and diffuse economic forces to democratic oversight and control."); Tim Wu, The Curse of Bigness: Antitrust in the New Gilded Age 9–11 (2018) (arguing that "[w]e have managed to recreate both the economics and politics of a century ago—the first Gilded Age—and remain in grave danger of repeating more of the signature errors of the twentieth century"); Lina Khan, The New Brandeis Movement: America's Antimonopoly Debate, 9 J. Eur. Competition L. & Prac. 131, 131–32 (2018) (discussing the historical roots and modern goals of the neo-Brandeisian movement); David McLaughlin, Forget Consumer Welfare. This Antitrust Movement Targets Power, Bloomberg Businessweek (Jan. 17, 2018), https://www.bloomberg.com/news/articles/2018-01-17/forget-consumer-welfare-this-antitrust-movement-targets-power-instead (on file with the *Columbia Law Review*) (describing the movement's goal as "not just to toughen enforcement by the federal government, but to return antitrust policy to its early 20th century roots to take on new corporate giants, particularly in the tech sector").

29. Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017).

30. See Ramon Ramirez, Elizabeth Warren Champions Michelob Ultra, Breaking Up Amazon at SXSW, Daily Dot (Mar. 9, 2019), https://www.dailydot.com/layer8/elizabeth-warren-john-kasich-sxsw/ [https://perma.cc/LK66-MVZJ] (describing Senator Elizabeth Warren's speech at SXSW in which she likened Amazon and Facebook "to the railroads under Roosevelt: 'The railroads were the place you had to be. . . . You had to get your wheat or your corn onto the railroads.'" (alteration in original) (quoting Sen. Elizabeth Warren)).

31. See, e.g., Australian Competition & Consumer Comm'n, Digital Platform Inquiry: Preliminary Report 4–5 (2018), https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Inquiry%20-%20Preliminary%20Report.pdf [https://perma.cc/F57Z-HG5S] (providing an overview of the "substantial market power" that Facebook and Google have in the Australian social media and online search markets, respectively); Autorité de la Concurrence & Bundeskartellamt, Competition Law and Data 11–16 (2016), http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddatafinal.pdf

have different business models, different value chains, and different primary markets. But one critical feature they share is the dual role they play in select markets: as both an operator of a dominant platform that hosts third-party merchants, content creators, or app developers, and as a market participant that competes with those same producers. This Part reviews some of the markets in which online platforms are integrated and the practices this integrated structure enables.

A. *Amazon*

Amazon provides a host of different services. It is the dominant online marketplace, the world's largest cloud computing service, a massive shipping and logistics network, a media producer and distributor, a grocer, a small-business lender, a live video-gaming streaming platform, a digital home assistant, a designer of apparel, and an online pharmacy.[32] Two areas where it both serves as a bottleneck facility and competes with those reliant on its bottleneck include online retail and digital home-assistant systems.

1. *Marketplace/AmazonBasics.* — In Amazon's early days, it operated primarily as an online retailer: It would procure goods at wholesale prices from suppliers and then sell them at retail prices to consumers. In 1999 it introduced Auctions, an online auctions service, and zShops, a fixed-price marketplace business—services that would evolve into the Amazon Marketplace, an open

---

[https://perma.cc/8KJG-RFTG] ("[T]he greater information resulting from expanded data collection, especially about competitors' pricing, may also be used by undertakings in ways that could limit competition."); Autorité de la Concurrence, Opinion No. 18-A-03 of 6 March 2018 on Data Processing in the Online Advertising Sector 2–10 (2018), http://www.autoritedelaconcurrence.fr/doc/avis18a03_en_.pdf [https://perma.cc/DVA5-FZ32] [hereinafter Data Processing in Online Advertising] (concluding that profits from growth in online advertising have mainly gone to just a handful of large firms and "those that are reaping the most rewards are companies that have access to vast sets of high-quality personal data"); Digital Competition Expert Panel, Unlocking Digital Competition 8–16 (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf [https://perma.cc/S8PP-H5TY] (providing twenty policy recommendations for how digital markets can be made more competitive); Digital, Culture, Media & Sport Comm., House of Commons, Disinformation and 'Fake News': Final Report 36 (2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf [https://perma.cc/9K7H-CZMB] (discussing how Facebook acquired immense amount of app-usage data from its customers and utilized this information to acquire companies that appeared profitable "or shut down those they judged to be a threat"); Select Comm. on Commc'ns, House of Lords, Regulating in a Digital World 45 (2019), https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf [https://perma.cc/YZP5-NP9W] ("Online communications platforms act as gatekeepers for the internet, controlling what users can access and how they behave. They can be compared to utilities in the sense that users feel they cannot do without them and so have limited choice but to accept their terms of service.").

32. For a full list of the lines of business in which Amazon operates, see Paris Martineau & Louise Matsakis, Why It's Hard to Escape Amazon's Long Reach, Wired (Dec. 23, 2018), https://www.wired.com/story/why-hard-escape-amazons-long-reach/ [https://perma.cc/HBH7-ZBCY].

platform on which other merchants could list their products to sell directly to consumers.[33] Unlike selling wholesale to Amazon, selling through the Marketplace permitted suppliers to maintain control over retail pricing and shipping.[34] Inviting producers to sell through Amazon Marketplace significantly expanded the catalogue of goods available on Amazon's platform, while freeing Amazon of the risk of purchasing inventory.[35]

This dramatic expansion in product selection has helped Amazon become the dominant online marketplace in the United States. The platform is estimated to capture 52.4% of all U.S. online retail spending[36] and 56.1% of the segment's traffic,[37] while 54% of all product searches originate on Amazon.[38] Amazon's share of ecommerce is more than double the market share of its next nine competitors combined,[39] and even merchants who list products on other sites can come to rely upon Amazon for up to 90% of their sales.[40] For many merchants, "Not being on Amazon doesn't feel like an option."[41]

---

33. Feng Zhu & Qihong Liu, Competing with Complementors: An Empirical Look at Amazon.com, 39 Strategic Mgmt. J. 2618, 2623–24 (2018); see also Lydia DePillis & Ivory Sherman, Amazon's Extraordinary Evolution: A Timeline, CNN (Oct. 4, 2018), https://www.cnn.com/interactive/2018/10/business/amazon-history-timeline/index.html [https://perma.cc/63P8-QBW8].

34. For a rundown of the tradeoffs between selling to Amazon as a vendor and selling on Amazon as a merchant, see Mary Weinstein, How to Sell on Amazon in 2019: A Complete Guide, CPC Strategy (Aug. 21, 2018), https://www.cpcstrategy.com/blog/2018/08/sell-on-amazon/ [https://perma.cc/2GKP-GNCX] (observing that the benefits of selling on Amazon include maintaining control over one's brand and pricing and receiving payments more quickly).

35. See Amazon, 2000 Amazon.com Annual Report 2 (2000), https://ir.aboutamazon.com/static-files/49b9a96d-f5ce-4695-a9a1-70eb8ffd3b87 [https://perma.cc/S6HV-BVW6].

36. Spencer Soper, Amazon Suppliers Panic Amid Purge Aimed at Boosting Profits, Bloomberg (Mar. 7, 2019), https://www.bloomberg.com/news/articles/2019-03-07/amazon-purges-suppliers-in-push-to-boost-e-commerce-profits? (on file with the *Columbia Law Review*) [hereinafter Soper, Amazon Suppliers Panic].

37. Leading Online Marketplace Websites in the United States as of 4th Quarter 2018, Based on Share of Visits, Statista, https://www.statista.com/statistics/270884/most-visited-websites-in-the-retail-sector-in-the-us/ [https://perma.cc/GR62-2U2P] (last visited Mar. 11, 2019); Ingrid Lunden, Amazon's Share of the US E-Commerce Market Is Now 49%, or 5% of All Retail Spend, TechCrunch (July 13, 2018), https://techcrunch.com/2018/07/13/amazons-share-of-the-us-e-commerce-market-is-now-49-or-5-of-all-retail-spend/ [https://perma.cc/AAZ7-A97Q] [hereinafter Lunden, Amazon's Share of the US E-Commerce Market].

38. Krista Garcia, More Product Searches Start on Amazon, eMarketer (Sept. 7, 2018), https://www.emarketer.com/content/more-product-searches-start-on-amazon [https://perma.cc/C5DP-U8LJ].

39. Its closest competitor, eBay, enjoys 6.6% of the ecommerce market, followed by Apple (3.9%) and Walmart (3.7%). Lunden, Amazon's Share of the US E-Commerce Market, supra note 37; see also Jeff Desjardins, Chart: Amazon's Dominance in Ecommerce, Visual Capitalist (Aug. 17, 2018), https://www.visualcapitalist.com/chart-shows-amazons-dominance-ecommerce/ [https://perma.cc/6B3S-4SMK]. For the purposes of antitrust analysis, the relevant product market is likely to be much narrower than "online retail."

40. Spencer Soper, Bezos Disputes Amazon's Market Power. But His Merchants Feel the Pinch, Bloomberg (Apr. 17, 2019), https://www.bloomberg.com/news/articles/2019-04-17/is-

Marketplace sales are a lucrative and booming part of Amazon's overall business. Amazon charges merchants either a $39.99 monthly subscription fee or a 99¢ per-item flat fee, depending on the plan, as well as a percentage of each transaction.[42] Analysts estimate that 52% of unit-goods[43] and 68% of total Amazon sales derived from Marketplace merchants in 2018.[44] The service fees Amazon charges third-party sellers generated $42.75 billion in 2018,[45] comprising around 18% of the company's net sales and its second-largest

amazon-too-powerful-its-merchants-are-starting-to-wonder (on file with the *Columbia Law Review*) [hereinafter Soper, Bezos Disputes].

41. Josh Dzieza, Prime and Punishment: Dirty Dealing in the $175 Billion Amazon Marketplace, Verge (Dec. 19, 2018), https://www.theverge.com/2018/12/19/18140799/amazon-marketplace-scams-seller-court-appeal-reinstatement [https://perma.cc/SW7Q-LGD2] (internal quotation marks omitted) (quoting Zac Plansky, an Amazon merchant); see also Bensinger, supra note 9; Angus Loten & Adam Janofsky, Sellers Need Amazon, but at What Cost?, Wall St. J. (Jan. 14, 2015), http://www.wsj.com/articles/sellers-need-amazon-but-at-what-cost-1421278220 (on file with the *Columbia Law Review*) ("'If you say no to Amazon, you're closing the door on tons of sales[.]' . . . 'You can't really be a high-volume seller online without being on Amazon, but sellers are very aware of the fact that Amazon is also their primary competitor.'" (quoting two Amazon merchants)); Stacy Mitchell, Amazon Doesn't Just Want to Dominate the Market—It Wants to Become the Market, Nation (Feb. 15, 2018), https://www.thenation.com/article/amazon-doesnt-just-want-to-dominate-the-market-it-wants-to-become-the-market/ [https://perma.cc/GV4R-475U] ("'If the customer is on Amazon, as a small business you have to say, "That is where I have to go[.]" . . . Otherwise, we are going to close our doors.'" (quoting an Amazon merchant)); Lara O'Reilly & Laura Stevens, Amazon, With Little Fanfare, Emerges as an Advertising Giant, Wall St. J. (Nov. 27, 2018), https://www.wsj.com/articles/amazon-with-little-fanfare-emerges-as-an-advertising-giant-1543248561 (on file with the *Columbia Law Review*) ("'They get all the prime real estate. It's unfair,' Mr. Boyce says, but 'we have to be on Amazon.'"). It is worth noting that, with Amazon's expansion into government procurement, even those merchants that traditionally sold directly to government agencies are being compelled onto Amazon's platform. See Olivia LaVecchia & Stacy Mitchell, Inst. for Local Self-Reliance, Amazon's Next Frontier: Your City's Purchasing 5 (2018), https://ilsr.org/wp-content/uploads/2018/07/ILSR_AmazonsNextFrontier_Final.pdf [https://perma.cc/S9H9-36WA] ("As Amazon sells the contract, it's told public officials that they can still shop with their local businesses but just do so through Amazon's platform.").

42. These sale percentage fees range from 3% to 45%, depending on the product category. See Selling on Amazon Fee Schedule, Amazon Seller Cent., https://sellercentral.amazon.com/gp/help/external/200336920/ref=asus_soa_p_fees?ld=NSGoogle [https://perma.cc/NU92-SJBQ] (last visited Mar. 25, 2019).

43. Eugene Kim, Amazon Added a First-Ever Warning About Counterfeit Products to Its Earnings Report, CNBC (Feb. 4, 2019), https://www.cnbc.com/2019/02/04/amazon-10k-warns-investors-about-counterfeit-problem-for-first-time.html [https://perma.cc/942C-V5G8]; Percentage of Paid Units Sold by Third-Party Sellers on Amazon Platform as of 4th Quarter 2018, Statista, https://www.statista.com/statistics/259782/third-party-seller-share-of-amazon-platform/ [https://perma.cc/SV74-6EY4] [hereinafter Statista, Third-Party Sellers] (last visited Mar. 11, 2019).

44. Juozas Kaziukenas, Amazon Marketplace Is the Largest Online Retailer, Marketplace Pulse (Dec. 3, 2018), https://www.marketplacepulse.com/articles/amazon-marketplace-is-the-largest-online-retailer [https://perma.cc/Y6W5-38BT].

45. Statista, Third-Party Sellers, supra note 43.

revenue segment.[46] Revenue from seller commissions is outpacing Amazon's overall online sales.[47]

In addition to serving as a major marketplace for third-party sellers, Amazon now also sells Amazon-branded goods on its platform. It first began offering private labels in 2009, primarily selling commodity goods such as batteries and HDMI cables.[48] In the decade since, its private-label business has expanded to include toys, shoes, apparel, jewelry, coffee, baby wipes, furniture, mattresses, vitamins, towels, and pet food, among other products.[49] Amazon has around 137 private-label brands—with just one of these brands accounting for over 1,500 distinct products.[50] Analysts estimate that Amazon's private-label sales amounted to $7.5 billion in 2018 and will reach $25 billion by 2022.[51]

Amazon exploits this dual role—marketplace operator and marketplace merchant—in two ways: first, by implementing Marketplace policies that privilege Amazon as a seller and give it greater control over brands and pricing, and, second, by appropriating the business information of third-party

---

46. Id.; see also Amazon.com, Inc., Annual Report (Form 10-K) 17 (Jan. 31, 2019) [hereinafter 2018 Amazon 10-K], https://www.sec.gov/Archives/edgar/data/1018724/000101872419000004/amzn-20181231x10k.htm [https://perma.cc/6UU4-WZMQ] (reporting that Amazon earned $232.89 billion in net sales in 2018).

47. Dzieza, supra note 41.

48. Kim, Amazon Is Doubling Down, supra note 9.

49. To see a continually updated database of Amazon's private labels, see TJI Amazon Brand Database, TJI Amazon Research, https://this.just.in/amazon-brand-database/ [https://perma.cc/SD2Y-8EKA] (last updated Mar. 11, 2019).

50. Id. As the database authors note, Amazon does not clearly delineate its private label brands or Amazon exclusive brands, leaving researchers to identify Amazon brands through trademark filings. Id. On its website, Amazon describes both private label and exclusive brands as "Our Brands." To give a sense of how many products may be sold under Amazon's own brand, in 2017 just *one* of these brands—AmazonBasics—covered 1,506 distinct products for sale. Mike Murphy, AmazonBasics Is Moving Well Beyond the Basics, Quartz (Dec. 14, 2017), https://qz.com/1155843/amazonbasics-is-moving-well-beyond-the-basics/ [https://perma.cc/VWW6-YRP7]. Amazon-exclusive brands—which are owned by third parties but sold exclusively on Amazon—number over 400. TJI Amazon Brand Database, supra note 49. Through its "Accelerator Program," Amazon recruits manufacturers to produce made-for-Amazon products. Eugene Kim, Amazon Quietly Launched a New 'Accelerator' Program to Create More Exclusive Brands for Its Website, CNBC (Oct. 4, 2018), https://www.cnbc.com/2018/10/04/amazon-quietly-launched-a-new-accelerator-program-to-create-more-brands-exclusively-sold-on-its-website.html [https://perma.cc/6RQM-QJJH]. Companies that join are granted access to marketing support and superior performance information. Id. Analysts say the program enables Amazon to "generate better profit margins," "control the supply chain for sourcing inventory," and "put more pressure on bigger brands to reduce their prices on Amazon to stay competitive." Id.

51. Eugene Kim, Amazon Has Been Promoting Its Own Products at the Bottom of Competitors' Listings, CNBC (Oct. 2, 2018), https://www.cnbc.com/2018/10/02/amazon-is-testing-a-new-feature-that-promotes-its-private-label-brands-inside-a-competitors-product-listing.html [https://perma.cc/S53B-YEAM] (citing investment research by Robinson Humphrey, which noted that "[p]rivate label is one of the highly under-appreciated trends within Amazon, in our view, which over time should give the company a strong 'unfair' competitive advantage").

merchants. One way that Amazon has favored Amazon goods and services is by presenting itself as the default seller even when Marketplace vendors have offered lower prices. A *ProPublica* investigation discovered that Amazon engineers its ranking algorithm to favor its own products as well as those sold by merchants that buy Amazon's fulfillment services.[52] Since an estimated 82% of Amazon sales go to the top listing—namely, whoever wins the Amazon "Buy Box"—this self-preferential treatment is an "oft-decisive advantage."[53] Amazon also appears to have privileged Amazon goods in promotional placements. According to *The Capitol Forum*, Amazon prioritizes its own clothing brands in its space for sponsored placements and appears to restrict competitors' access to this placement, directing consumers toward its own products over those sold by rivals.[54] Even when a customer goes on a Marketplace merchant's product page, Amazon will show prominent ads and pop-ups directing customers to Amazon's own products instead.[55]

A second way Amazon has favored itself as a seller is through implementing Marketplace policies that enable it to become the exclusive merchant of certain products. According to news reports, Amazon encourages brands to sell directly to Amazon in exchange for Amazon's commitment to enforce the brand's minimum advertised prices (MAP) on Amazon.[56] Enforcing this policy, Amazon expels any third parties selling lower than the MAP,

---

52. See Julia Angwin & Surya Mattu, Amazon Says It Puts Customers First. But Its Pricing Algorithm Doesn't, ProPublica (Sept. 20, 2016), https://www.propublica.org/article/amazon-says-it-puts-customers-first-but-its-pricing-algorithm-doesnt [https://perma.cc/8DVN-CTDT] ("[Amazon] appears to be using its market power and proprietary algorithm to advantage itself at the expense of sellers and many customers."); see also Zhu & Liu, supra note 33, at 2637 ("We observe across many instances of entry that Amazon may present itself as the default seller even when the same product is offered at lower cost (i.e., product price plus shipping cost), with a comparable shipping speed by third-party sellers with high ratings."). By omitting shipping costs for these Amazon-affiliated products, Amazon gives these items top placement in search results. Angwin & Mattu, supra.

53. Id.

54. Amazon: By Prioritizing Its Own Fashion Label Brands in Product Placement on Its Increasingly Dominant Platform, Amazon Risks Antitrust Enforcement by a Trump Administration, The Capitol Forum (Dec. 13, 2016), https://thecapitolforum.com/wp-content/uploads/2016/07/Amazon-2016.12.13.pdf (on file with the *Columbia Law Review*) [hereinafter The Capitol Forum, Amazon Prioritizing]; see also Creswell, supra note 9 (discussing how Amazon uses its data advantage "to steer shoppers toward its in-house brands and away from its competitors"). More recent analysis by L2 found that, while Amazon is investing significantly in advertising its brands on Amazon, it owns approximately 15% of the sponsored placement for certain clothing-related keywords. See Cooper Smith, Amazon's Private Label Fever, L2 Inc (Apr. 3, 2018), https://www.l2inc.com/daily-insights/amazons-private-label-fever [https://perma.cc/WGK2-GXL8] (noting that Amazon Essentials owns 16% of the sponsored placements for keywords related to dress shirts and 13% for polo shirts).

55. O'Reilly & Stevens, supra note 41.

56. Amazon Ousted Marketplace Sellers in Order to Be Only Seller of Certain Products; A Closer Look at Monopolization Enforcement, The Capitol Forum (Jan. 23, 2018) (on file with the *Columbia Law Review*) [hereinafter The Capitol Forum, Ousted Marketplace Sellers].

sometimes leaving Amazon as the only remaining seller.[57] Last November, Amazon also signed a deal to become an authorized reseller of Apple's devices—an agreement that prompted Amazon to delist any Apple products sold by Marketplace merchants who are not authorized Apple resellers.[58] Since one of the requirements for becoming an authorized Apple reseller includes purchasing a certain minimum amount of product directly from Apple, most independent merchants will no longer be able to sell Apple products on Amazon.[59]

Another policy change Amazon has instituted is requiring certain brands on Marketplace to instead sell wholesale to Amazon—granting Amazon the ability to set the retail price and maintain exclusive access to certain sales and customer data.[60]

---

57. Id. While Amazon enforces MAP agreements that it has entered into with brands, it also overrides pricing decisions by third-party merchants in ways that could place them in violation of merchant's MAP agreements. Laura Stevens, Amazon Snips Prices on Other Sellers' Items Ahead of Holiday Onslaught, Wall St. J. (Nov. 5, 2017), https://www.wsj.com/articles/amazon-snips-prices-on-other-sellers-items-ahead-of-holiday-onslaught-1509883201 (on file with the *Columbia Law Review*) (reporting that Amazon lowers prices on products offered by independent merchants, which "could inadvertently violate a merchant's agreement with a brand to keep its products at or above a set minimum advertised price"). In one instance, Amazon used this strategy to become the only merchant on Amazon to sell a particular type of replacement water filter. Prior to Amazon's initiation of the MAP, up to thirty sellers competed in the market for this replacement water filter. Since becoming the sole merchant of these filters on Amazon, the company has steadily raised prices. The Capitol Forum, Ousted Marketplace Sellers, supra note 56.

58. Ben Fox Rubin, How Amazon's Deal with Apple Puts the Hurt on Small Sellers, CNET (Nov. 19, 2018), https://www.cnet.com/news/how-amazons-deal-with-apple-puts-the-hurt-on-small-sellers/ (on file with the *Columbia Law Review*).

59. Sam Medley, Amazon Will Prevent Unauthorized Third-Parties from Selling Apple Products Through Its Online Store, Notebook Check (Nov. 11, 2018), https://www.notebookcheck.net/Amazon-will-prevent-unauthorized-third-parties-from-selling-Apple-products-through-its-online-store.359521.0.html [https://perma.cc/2PTQ-LPRQ].

60. See Jason Del Rey, An Amazon Revolt Could Be Brewing as the Tech Giant Exerts More Control over Brands, Recode (Nov. 29, 2018), https://www.recode.net/2018/11/29/18023132/amazon-brand-policy-changes-marketplace-control-one-vendor [https://perma.cc/9EJ8-ZW9A] ("Over the past few months, Amazon has applied intense pressure to consumer brands across different product categories—seizing more control over what, where and how they can sell their goods on the so-called everything store, these people say."). By assuming control over pricing, Amazon can use brands' products to experiment and determine the optimal price—information it can use when rolling out its own private label version.

For some sellers, however, Amazon's policy change has gone in the other direction. In March, Amazon abruptly informed thousands of vendors that it would no longer place orders for their items. Some were explicitly told that in order to keep selling on Amazon, they would need to establish merchant accounts and sell on the Marketplace instead. Id. Jason Del Rey, Amazon Ousted Thousands of Merchants with No Notice—Showing the Danger of Relying on the Shopping Platform, Recode (Mar. 8, 2019), https://www.recode.net/2019/3/8/18252606/amazon-vendors-no-orders-marketplace-counterfeits [https://perma.cc/664D-G4DW]; see also Soper, Amazon Suppliers Panic, supra note 36 ("'If you're heavily reliant on Amazon, which a lot of these vendors are, you're in a lot of trouble,' said Dan Brownsher, Chief Executive Officer of Channel Key, a Las Vegas e-commerce consulting business . . . . 'If this goes on, it can put people out of business.'").

In theory, efforts by Amazon to enter exclusive or semiexclusive agreements with brands could be understood as an effort by Amazon to combat counterfeits, which proliferate on Amazon.[61] But in practice, Amazon also seems to use its ability to decide whether or not to police counterfeits as leverage against brands who might otherwise refrain from selling on Amazon.[62] Nike, for example, for years refused to list its products on Amazon. Faced with a situation where merchants were selling both authentic and fake Nike goods on Marketplace anyway, Nike ultimately signed an agreement to sell wholesale to Amazon in exchange for stricter policing of counterfeits.[63] An executive from Birkenstock—which stopped supplying products to Amazon in 2017—stated that the only way a brand or supplier can get Amazon to fully commit to policing counterfeits is to sell its entire catalogue to Amazon.[64] Even as Amazon professes a "zero tolerance" policy for counterfeit products,[65] reports suggest that not only has the company "resisted calls to do more to police its site," but that it has "thrived" from this practice, given the additional leverage

61. One advocacy group that identifies fake goods has identified around 58,000 counterfeits on Amazon. Edgar Alvarez, Amazon Needs to Get a Handle on Its Counterfeit Problem, EndGadget (May 31, 2018), https://www.engadget.com/2018/05/31/fulfilled-by-amazon-counterfeit-fake/ [https://perma.cc/2EN6-JE7H]. Apple is among the companies that have sued third-party Amazon sellers for selling counterfeit products, and Apple has also criticized Amazon for hosting those products. See Gregg Keizer, Apple Sues Amazon Supplier over Fake iPhone Chargers, Computerworld (Oct. 20, 2016), https://www.computerworld.com/article/3133627/apple-sues-amazon-supplier-over-fake-iphone-chargers.html [https://perma.cc/PD6N-V5G5].

62. See Laura Stevens & Sara Germano, Nike Thought It Didn't Need Amazon. Then the Ground Shifted, Wall St. J. (June 28, 2017), https://www.wsj.com/articles/how-nike-resisted-amazons-dominance-for-years-and-finally-capitulated-1498662435 (on file with the *Columbia Law Review*) ("Nike agreed to start selling some products directly to Amazon in exchange for stricter policing of counterfeits and restrictions on unsanctioned sales . . . ."); see also David Pierson, Extra Inventory. More Sales. Lower Prices. How Counterfeits Benefit Amazon, L.A. Times (Sept. 28, 2018), https://www.latimes.com/business/technology/la-fi-tn-amazon-counterfeits-20180928-story.html [https://perma.cc/5ETX-UNFJ] ("Not only has the platform avoided any serious backlash for allowing the sale of fake goods, it's actually thrived from it, say more than two dozen brand owners, e-commerce consultants, attorneys, investigators and public policy experts.").

63. Stevens & Germano, supra note 62.

64. Ari Levy, Birkenstock Quits Amazon in US After Counterfeits Surge, CNBC (July 20, 2016), https://www.cnbc.com/2016/07/20/birkenstock-quits-amazon-in-us-after-counterfeit-surge.html [https://perma.cc/TZ7H-QBFA] ("The only way to get Amazon's support in creating a clean environment, according to [Birkenstock CEO David] Kahan, is by selling the entire catalog to Amazon. . . . Plenty of brands have opted to team up with Amazon and hand over full collections instead of engaging in a never-ending fight.").

65. Amazon's Anti-Counterfeiting Policy states: "Products offered for sale on Amazon must be authentic. The sale of counterfeit products is strictly prohibited. Failure to abide by this policy may result in loss of selling privileges, funds being withheld, and destruction of inventory in our possession." Amazon Anti-Counterfeiting Policy, Amazon Seller Cent., https://sellercentral.amazon.com/gp/help/external/201165970 [https://perma.cc/F36B-X4SV] (last visited Mar. 13, 2019). In 2018, Amazon listed counterfeits as a "risk factor" in its 10-K. See 2018 Amazon 10-K, supra note 46, at 14.

that counterfeiters give Amazon over brands and merchants.[66] Indeed, sellers confronting any host of difficulties on Amazon's site—ranging from abrupt account suspensions to sabotage campaigns by rivals—soon learn that "the solution is often to more fully meld with Amazon" in ways that provide Amazon with more revenue, more control, or greater access to a merchant's sensitive business information.[67] Earlier this year, Amazon announced that sellers looking to fight counterfeiters and manage other problems on its platform could purchase a new service from Amazon for $30,000 to $60,000 a year.[68] The rapid growth of Amazon's digital ad business suggests brands may increasingly need to buy advertising in order to attract more customer clicks.[69]

Separate from policies that explicitly or implicitly require merchants and vendors to buy additional Amazon services, sellers worry about subtler forms of discrimination. There are numerous means by which Amazon can disfavor any particular merchant: It can suspend or shut down accounts overnight, withhold merchant funds, change page displays, and throttle or block favorable reviews.[70]

In addition to implementing Marketplace policies that favor Amazon's direct sales, Amazon appropriates Marketplace merchants' data to shape its

66. Pierson, supra note 62. Sellers note that Amazon's decision to "openly court Chinese manufacturers, weaving them intimately into the company's expansive logistics operation" has made the counterfeiting problem worse. Sales by China-based merchants on Amazon more than doubled in 2015. Ari Levy, Amazon's Chinese Counterfeit Problem Is Getting Worse, CNBC (July 8, 2016), https://www.cnbc.com/2016/07/08/amazons-chinese-counterfeit-problem-is-getting-worse.html [https://perma.cc/2V2Q-JNRK]. Lawsuits by Daimler and Williams-Sonoma have alleged that even products sold directly by Amazon are infringing upon intellectual property. Complaint for Damages and Injunctive Relief at 6–16, Williams-Sonoma, Inc. v. Amazon.com, Inc., No. 18-cv-07548 (N.D. Cal. filed Dec. 14, 2018) (accusing Amazon of improperly displaying the "Williams-Sonoma" trademark on its website and of violating a patent owned by Williams-Sonoma); Complaint for Trademark Infringement at 11–16, Daimler AG vs. Amazon.com, Inc., No. 17-cv-7674 (C.D. Cal. filed Oct. 20, 2017) (alleging that Amazon had infringed on Daimler trademarks by selling wheel center caps with the Mercedes-Benz logo).

67. Dzieza, supra note 41.

68. Eugene Kim, Amazon Is Inviting Sellers to Private Meetings at CES to Promote a Premium Support Service that Costs Up to $60,000 a Year, CNBC (Jan. 9, 2019), https://www.cnbc.com/2019/01/09/amazon-holds-ces-meetings-with-marketplace-sellers-promoting-support.html [https://perma.cc/S78N-X27R].

69. See O'Reilly & Stevens, supra note 41 ("Amazon's ad business now contributes to gross profit and is expected to generate more income than its cloud business—which currently provides the bulk of its profits—as soon as 2021 . . . ."). Some Marketplace merchants respond to direct competition with Amazon on Amazon by purchasing hundreds of thousands of dollars of advertisements every year. See Soper, Bezos Disputes, supra note 40 ("Jason Boyce, having navigated Planet Amazon for 15 years, is selling his business and has started a consulting firm helping other merchants. . . . [H]e says the money he was forced to spend to advertise his products reduced his profits by several hundred thousand dollars a year.").

70. See Andrew Buck, Is Amazon Deleting or Blocking Your Reviews?, LandingCube (Jan. 4, 2019), https://landingcube.com/amazon-deleting-reviews/ [https://perma.cc/Y4SJ-WN4V]; Dzieza, supra note 41 ("For sellers, Amazon is a quasi-state. They rely on its infrastructure—its warehouses, shipping network, financial systems, and portal to millions of customers—and pay taxes in the form of fees. They also live in terror of its rules, which often change and are harshly enforced.").

own retail strategy. By virtue of hosting a digital marketplace, Amazon's ability to collect and analyze ecommerce data is unrivaled. While even large brick-and-mortar stores can track consumer purchase histories and brand sales, the information Amazon harvests is far more sophisticated and precise.[71] In addition to tracking overall trends, it captures which goods a customer clicked on but did not buy, the exact price change that induced a customer to peruse an item or purchase it, how long a user hovers her mouse over a particular good, how customers are reacting to product images and videos, and a wealth of other microdetails that add up to a formidable—and constantly evolving—arsenal of market intelligence.[72] It is as if a shopping mall tracked not only all the foot traffic into a store, but also which items caught a customer's glance, which products made it into the shopping cart but were never purchased, as well as complete transaction and revenue data and all customer reviews. All of this information is gathered not just on products Amazon sells but also on third-party merchants,[73] giving Amazon an unprecedented vantage point over 50% of ecommerce in the United States.[74]

Reports suggest Amazon uses this trove of Marketplace data to inform both its retail business and its private labels. In some cases, Amazon has responded to popular items introduced by third-party merchants by sourcing those same products directly from the manufacturer and demoting the third-party merchants in search results.[75] One study found that in the case of women's clothing, Amazon "began selling 25 percent of the top items first sold through marketplace vendors."[76] Its private label, meanwhile, has also closely tracked successful Marketplace items. While AmazonBasics—Amazon's private-label brand—initially focused on generic goods like batteries and blank

71. See Allie Gray Freeland, Inside Amazon's Approach to Data and People-Based Marketing, LiveIntent (Apr. 24, 2018), https://blog.liveintent.com/amazon-data-people-based-marketing/ [https://perma.cc/2BAU-XDF2] (describing "Amazon's peerless data bank of search and online purchasing behavior, mined from its hundreds of millions of customers").

72. See id. It can identify whether a customer lands on Amazon after visiting a rival website and can track customer behavior through email—whether a customer viewed, clicked, forwarded, or bought an item in a marketing email, or whether she preferred a similar product within that email. Id.

73. See George Anderson, Is Amazon Undercutting Third-Party Sellers Using Their Own Data?, Forbes (Oct. 30, 2014), http://www.forbes.com/sites/retailwire/2014/10/30/is-amazon-undercutting-third-party-sellers-using-their-own-data [https://perma.cc/KK5Q-V78R].

74. See supra notes 36–41 and accompanying text.

75. See Bensinger, supra note 9 ("[S]ome sellers say they suspect Amazon uses sales data from outside merchants to make purchasing decisions in order to undercut them on price and give items featured placement under a given search . . . ."). For a specific example, take the case of Pillow Pets, "stuffed-animal pillows modeled after NFL mascots" that a third-party merchant sold through Amazon's site. Id. For several months, the merchant sold up to one hundred pillows per day. Id. According to one account, "just ahead of the holiday season . . . , [the merchant] noticed Amazon had itself begun offering the same Pillow Pets for the same price while giving [its own] products featured placement on the site." Id. The merchant's own sales dropped to twenty per day. Id.

76. Anderson, supra note 73.

DVDs, it has since expanded into a much broader array of products.[77] For a few years "the house brand 'slept quietly as it retained data about other sellers' successes.'"[78] As Amazon now rolls out more AmazonBasics products, it is clear that the company has used "insights gleaned from its vast Web store to build a private-label juggernaut that now includes more than 3,000 products."[79]

Initial empirical work suggests that Amazon's entry into competition with third-party merchants does not affect product price or customer satisfaction but does dissuade third-party sellers from continuing to offer the product.[80] Merchants, especially small ones, "are discouraged from growing their business on the platform."[81]

2. *Alexa/Alexa Devices/Alexa Skills*. — Another area in which Amazon both serves as a primary platform and competes with platform services is the voice computing market. Amazon jump-started the voice assistant market in 2015 when it publicly rolled out the Echo, its smart speaker, embedded with Alexa, the artificial intelligence software that serves as a voice assistant.[82] An early mover in this market, Amazon remains dominant.[83]

The applications that power Alexa—that enable it to perform particular tasks—are called "skills."[84] Skills execute various requests: They can dim your kitchen lights, offer recipe ideas, and provide allergy forecasts with precise

---

77. Spencer Soper, Got a Hot Seller on Amazon? Prepare for E-Tailer to Make One Too, Bloomberg (Apr. 20, 2016), https://www.bloomberg.com/news/articles/2016-04-20/got-a-hot-seller-on-amazon-prepare-for-e-tailer-to-make-one-too (on file with the *Columbia Law Review*).

78. Id. (quoting a report provided exclusively to Bloomberg News).

79. Id.

80. Zhu & Liu, supra note 33, at 2634.

81. Id.

82. See Farhad Manjoo, The Echo from Amazon Brims with Groundbreaking Promise, N.Y. Times (Mar. 9, 2016), https://www.nytimes.com/2016/03/10/technology/the-echo-from-amazon-brims-with-groundbreaking-promise.html (on file with the *Columbia Law Review*).

83. The Echo captured close to 67% of the smart speaker market in 2018, Ingrid Lunden, eMarketer: Amazon Took 2/3 of Smart Speaker Sales in 2018, but Echo Will Face the Squeeze in 2019, TechCrunch (Dec. 20, 2018), https://techcrunch.com/2018/12/20/fading-echo/ [https://perma.cc/MA5P-8VDW], and as of 2017, Alexa powered 68% of smart speakers in the United States. Rayna Hollander, Amazon's Alexa Is Dominating the Smart Speaker Landscape, Bus. Insider (Oct. 13, 2017), https://www.businessinsider.com/amazon-alexa-smart-speaker-landscape-2017-10 (on file with the *Columbia Law Review*). As of January 2019, Amazon has sold more than 100 million devices with Alexa, more than 150 products have Alexa built in, and more than 28,000 smart-home devices are now compatible with Alexa. Dieter Bohn, Amazon Says 100 Million Alexa Devices Have Been Sold—What's Next?, Verge (Jan. 4, 2019), https://www.theverge.com/2019/1/4/18168565/amazon-alexa-devices-how-many-sold-number-100-million-dave-limp [https://perma.cc/972N-EE3J].

84. See James Stables, The Best Amazon Alexa Skills for Your Echo Smart Speakers, Ambient (Mar. 13, 2019), https://www.the-ambient.com/guides/best-amazon-alexa-skills-187 [https://perma.cc/6SEM-WHU3]. To analogize with the smart phone market, imagine Echo as the hardware (iPhone), Alexa as the operating system (iOS), Alexa first domains as built-in apps (Apple Music), and skills as independent apps (Spotify).

pollen counts.[85] Skills are created by third-party developers, who have built over 80,000 skills for Alexa.[86] Meanwhile, a host of manufacturers have produced Alexa-compatible devices or appliances.[87]

While third-party skills developers and manufacturers are critical to expanding the Alexa ecosystem, Amazon also actively competes with both.[88] Amazon has recently introduced dozens of new features and devices, including an Alexa-enabled microwave, security camera, subwoofer, and smart plug—smart devices that existing Amazon partners had already been providing.[89] Given how Amazon uses Marketplace data,[90] it seems reasonable to assume that Amazon uses its retail platform for insight into sales of current smart devices, which then informs its production strategy. In 2015, Amazon launched the $100 million Alexa Fund, which supports voice-technology startups and was designed to help cultivate a "developer ecosystem" around Alexa.[91] Some observers, however, say that Amazon is using the fund to mine product ideas that it then produces itself.[92] Nucleus, for example—a startup that had received backing from the Alexa Fund to create a voice-controlled video device—went on to watch Amazon release an almost identical product.[93] While startups backed by the Alexa Fund sometimes get unique access to Amazon, some investors advise businesses "to be wary of accepting Amazon's investment, because of the risk of Amazon copying ideas."[94] Following allegations that Amazon appropriates from its portfolio companies, Amazon has privately

85. See id.

86. Matt Day, Amazon's Alexa Has 80,000 Apps—and No Runaway Hit, Bloomberg (Mar. 11, 2019), https://www.bloomberg.com/news/articles/2019-03-11/amazon-s-alexa-has-80-000-apps-and-no-runaway-hit (on file with the *Columbia Law Review*).

87. See Bohn, supra note 83 (estimating that 4,500 different manufacturers have produced Alexa-compatible devices).

88. See Ben Fox Rubin, Amazon's Gadget Battle with Google Could Upend Its Alexa Allies, CNET (Oct. 5, 2018), https://www.cnet.com/news/amazons-gadget-battle-with-google-could-upend-its-alexa-allies/ (on file with the *Columbia Law Review*) ("These new Amazon devices serve as more examples of Amazon simultaneously cooperating with and competing against its partners as it creates more devices for its Alexa voice assistant.").

89. Id.; Nick Statt, Amazon Wants Alexa to Be the Operating System for Your Life, Verge (Sept. 27, 2018), https://www.theverge.com/2018/9/27/17911300/amazon-alexa-echo-smart-home-eco-system-competition [https://perma.cc/U3RJ-CD9R].

90. See supra notes 75–79 and accompanying text.

91. Patience Haggin, Startups Weigh Pros, Cons of Alexa Fund, Wall St. J. (Aug. 28, 2017), https://www.wsj.com/articles/startups-weigh-pros-cons-of-alexa-fund-1503919800 (on file with the *Columbia Law Review*).

92. See, e.g., id. (expressing a concern held by some venture capitalists that Amazon might copy ideas generated by Alexa Fund startups).

93. Jason Del Rey, Amazon Invested Millions in the Startup Nucleus—Then Cloned Its Product for the New Echo, Recode (May 10, 2017), https://www.recode.net/2017/5/10/15602814/amazon-invested-startup-nucleus-cloned-alexa-echo-show-voice-control-touchscreen-video [https://perma.cc/PUE6-QYKK] (quoting Alexa Fund representatives).

94. Haggin, supra note 91.

reached out to startups to mitigate those concerns, saying that a "clear 'firewall' exists between the Alexa Fund and Amazon's product development teams."[95]

Amazon also competes with Alexa-skills developers. From its rollout, Alexa has had some built-in features, such as weather and timers.[96] It regularly introduces new features, which sometimes offer the same service as an existing skill or tool provided by third parties.[97] Three areas in which Alexa has entered into direct competition with third-party skill providers are analytics, testing tools, and Blueprints.[98]

The primary advantage that Alexa domains enjoy over third-party skills is that they are set as the default. If a user asks a question that both an Alexa-native and a third-party skill can answer, the default skill activated will be the one native to the Alexa engine.[99] This default setting can be justified as way to offer users a smoother experience and to solve the technical problem of knowing where to send a request. But the effect is to create a built-in bias to steer users toward Alexa domains over third-party skills. Recent announcements suggest that Amazon is looking to enable the surfacing of skills into the first domain, which would mean Alexa would be able to sort through its abilities to activate the one that best addressed a user's request.[100] While, in

---

95. Eugene Kim, Amazon Wants to Invest in Start-Ups, but Some Are Nervous About Taking the Money, CNBC (Sept. 13, 2017), https://www.cnbc.com/2017/09/13/amazon-reassured-alexa-fund-start-ups-about-competition.html [https://perma.cc/6FK8-RY2T].

96. See, e.g., Dave Smith, I've Owned an Amazon Echo for Nearly a Year Now—Here Are My 19 Favorite Features, Bus. Insider (Oct. 5, 2016), https://www.businessinsider.com/amazon-echo-features-2016-10 (on file with the *Columbia Law Review*).

97. See supra notes 88–89 and accompanying text.

98. See John Koetsier, Analytics for AI Assistants: VoiceLabs Reveals Vital Stats for Alexa Skills and Google Actions, VentureBeat (Dec. 8, 2016), https://venturebeat.com/2016/12/08/analytics-for-ai-assistants-voicelabs-reveals-vital-stats-for-alexa-skills-and-google-actions/ [https://perma.cc/8QDG-QGYW]; see also About Us, Bespoken, https://bespoken.io/about/ [https://perma.cc/7M27-2U4A] (last visited Apr. 1, 2019) (describing Bespoken's work providing "testing and monitoring for voice apps"); Kaiyin Hu, Unit Testing: Creating Functional Alexa Skills, Amazon Alexa: Alexa Blogs (Aug. 7, 2018), https://developer.amazon.com/blogs/alexa/post/35bdad3d-57c8-4623-88c6-815540697af5/unit-testing-create-functional-alexa-skills [https://perma.cc/EC4G-HQFN] (reporting Amazon's announcement that it is building its own monitoring tools); Sarah Perez, Amazon's 'Alexa Blueprints' Can Now Be Published Publicly on the US Alexa Skills Store, TechCrunch (Feb. 13, 2019), https://techcrunch.com/2019/02/13/amazon-opens-its-us-alexa-skill-store-to-non-developers/ [https://perma.cc/T62E-Y9KG].

99. For example, if a user says, "Alexa, tell me the weather," Alexa will summon its built-in weather feature. In order to access, say, Big Sky, a third-party weather skill, a user would need to say, "Alexa, ask Big Sky for the weather." See Taylor Martin, How to Get Better Weather Forecasts on Your Alexa Speaker, CNET (July 17, 2017), https://www.cnet.com/how-to/how-to-get-better-weather-forecasts-on-your-alexa-speaker/ (on file with the *Columbia Law Review*).

100. See Monica Chin, Amazon Is Killing the Skill (as We Know It), Tom's Guide (Sept. 13, 2018), https://www.tomsguide.com/us/amazon-alexa-kills-skills,news-28072.html [https://perma.cc/J2HG-4G42] ("[Y]ou won't need to say 'Get me an Uber,' you'll say, 'Get me a car to the airport.' Amazon's assistant will use context clues, such as your location, your

theory, this could place a third-party skill on equal footing with an Alexa domain, the transition could also strengthen Alexa's role as a gatekeeper, rendering skills more captive to Amazon's discretion.

Amazon closely tracks usage patterns on Alexa.[101] It also enjoys exclusive access to the voice data that Alexa collects—data that capture the questions consumers ask voice platforms.[102] Alexa maintains access to this data even when the information is collected through third-party skills, and Amazon can use the information to both steer its future moves in the voice-assistant market and enrich other parts of its business, such as advertising.[103] This unique dataset will also give Amazon a huge advantage in continuing to develop its machine learning.

No empirical work has closely examined what guides Alexa's entry into certain skills or devices or how the threat of direct competition with Alexa affects third-party developers.

B. *Alphabet*

Alphabet, the parent company of Google, is a conglomerate comprised of subsidiaries in digital advertising, internet services, artificial intelligence, biotech, broadband, and venture capital.[104] Google—which encompasses digital advertising, Android, Chrome, Google Cloud, Google Maps, Google Play, Google Search, hardware, search, and YouTube[105]—remains the entity's profit center. In 2018, Google pulled in $36.5 billion in operating income, while the combined total of Alphabet's other segments posted a loss.[106]

There are several markets in which Google both serves as a major platform and competes with platform participants. These include generalized search, Android operating system/apps, and its online ad exchange. Although Google's integrations in the smartphone and online advertising markets have

---

subscriptions and services you've used in the past, to determine whether to call an Uber, Lyft, or other ride-sharing service.").

101. Amazon is seeking to dramatically expand the data it collects from third-party gadgets, asking them to report, for example, not just when a television is on but what channel it is set to. Matt Day, Your Smart Light Can Tell Amazon and Google When You Go to Bed, Bloomberg (Feb. 12, 2019), https://www.bloomberg.com/news/articles/2019-02-12/your-smart-light-can-tell-amazon-and-google-when-you-go-to-bed (on file with the *Columbia Law Review*).

102. Drew Firment, Alexa Data Analytics Are a Gold Mine, A Cloud Guru (Feb. 12, 2017), https://read.acloud.guru/alexa-data-analytics-are-a-gold-mine-b4ceb02526d2 [https://perma.cc/D9K3-9WFW].

103. See id. ("For example, if someone asks 'Alexa, what are the signs of pregnancy'—the customer should also expect to see diapers as an item on their suggested wish-list the next time they go shopping on Amazon.").

104. See Avery Hartmans, All the Companies and Divisions Under Google's Parent Company, Alphabet, Bus. Insider (Dec. 13, 2018), https://www.businessinsider.com/alphabet-google-company-list-2017-4 (on file with the *Columbia Law Review*).

105. See id.

106. Alphabet Inc., Annual Report (Form 10-K) 81 (Feb. 4, 2019) [hereinafter 2018 Alphabet 10-K], https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm [https://perma.cc/C2YS-QXCE].

also attracted antitrust attention, this section focuses on Google's integration in search.

1. *Google Search/Google Verticals.* — Google is a dominant internet search company, capturing around 88% of the U.S. search engine market[107] and 95% of mobile searches.[108] It began as a general search provider, indexing the web and developing algorithms to identify which web content may provide a relevant response to a user's search query. Search users do not pay money for their searches; instead, Google collects and analyzes data about users to sell targeted advertisements. In 2018, ad sales constituted 85% of all Alphabet revenue.[109]

The search engine market is comprised of "horizontal" search—a general search engine that offers results regardless of subject area—and "vertical" search, which limits query results to a specific category of content.[110] Even as Google became the dominant website for horizontal search, a stable of independent entities launched their own specialized search engines, focused on areas like comparison shopping, local search, flight search, and financial data.[111] Because Google is the dominant provider of online search, this ecosystem of vertical sites relies on Google to be seen and discovered by users.[112]

---

107. Search Engine Market Share in United States of America, StatCounter, http://gs.statcounter.com/search-engine-market-share/all/united-states-of-america [https://perma.cc/WQ2M-ZUAY] (last updated Mar. 2019). The remaining share of the market is split between Bing (6%), Yahoo! (4%), and DuckDuckGo (1%). Id. Globally, Google captures 92%, with Bing (2%), Yahoo! (2%), and Baidu (1%) following. Search Engine Market Share Worldwide, StatCounter, http://gs.statcounter.com/search-engine-market-share [https://perma.cc/VHA3-HBH7] (last updated Mar. 2019).

108. Mobile Search Engine Market Share in United States of America, StatCounter, http://gs.statcounter.com/search-engine-market-share/mobile/united-states-of-america [https://perma.cc/9JT8-DN8J] (last updated Mar. 2019). Google products also capture 59% of the web browser market. Google Embraces Ad-Blocking via Chrome, Economist (Feb. 17, 2018), https://www.economist.com/business/2018/02/17/google-embraces-ad-blocking-via-chrome (on file with the *Columbia Law Review*). Google captures 81% of the U.S. online maps market. Google Maps API, Datanyze, https://www.datanyze.com/market-share/mapping-and-gis/google-maps-api-market-share (on file with the *Columbia Law Review*) (last visited Apr. 3, 2019). It captures 77% of the internet video market. Online Video Platforms, Datanyze, https://www.datanyze.com/market-share/online-video (on file with the *Columbia Law Review*) (last visited Apr. 3, 2019). And it captures 88% of the global market for mobile operating systems. Global Market Share Held by the Leading Smartphone Operating Systems in Sales to End Users from 1st Quarter 2009 to 2nd Quarter 2018, Statista, https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/ (on file with the *Columbia Law Review*) (last visited Apr. 3, 2019).

109. See 2018 Alphabet 10-K, supra note 106, at 7.

110. See Jim Yu, Search Is More than Google: Mastering Vertical Search Optimization, Search Engine Land (May 15, 2018), https://searchengineland.com/search-is-more-than-google-mastering-vertical-search-optimization-298123 [https://perma.cc/FPW4-FL98].

111. See, e.g., Adam Vincenzini, 30 Specialized Search Engines Focused on Specific Content, Next Web (Apr. 29, 2012), https://thenextweb.com/lifehacks/2012/04/29/30-specialist-and-super-smart-search-engines/ [https://perma.cc/83SF-4LV5].

112. See supra notes 107–108 and accompanying text.

Although Google introduced its first vertical product around 2002,[113] only in 2005 did it begin strategically investing in and promoting additional vertical properties, including in local search, finance, and travel.[114] Its foray into these areas rendered standalone vertical properties, such as Yelp and TripAdvisor, dependent on their biggest rival.[115]

Google took advantage of this dual role in several ways—conduct that the Federal Trade Commission (FTC) investigated as part of an antitrust probe in 2011. As revealed by an FTC staff memorandum that was partially and inadvertently disclosed to the *Wall Street Journal* in 2015, the investigation found that Google used its position in general search both to give its vertical properties preferential treatment and to appropriate content from third-party competitors in vertical search.[116]

According to FTC staff from the Bureau of Competition (BC), Google rolled out a new interface—"Universal Search"—to privilege Google content and demote third-party content.[117] It relied on a host of tactics. For one, Google displayed Universal Search results at or near the top of its search engine ranking page, which had the effect of demoting and resulting in "significant loss of traffic" to many vertical rivals.[118] Google also "embellished" its vertical results with "eye-catching interfaces" that helped steer users to Google's vertical properties—interfaces that Google did not make available to competitor vertical websites.[119] Commission staff concluded that Google's self-privileging had been at least partially motivated by fear that superior vertical competitors would divert search queries—and, subsequently, advertisement dollars—from Google.[120] The tactic worked: Self-preferential treatment "led to gains in user share for its own properties."[121]

---

113. See Wired Staff, Google Gets Its Groove On, Wired (Mar. 29, 2004), https://www.wired.com/2004/03/google-gets-its-groove-on/ [https://perma.cc/PL8U-5X5A].

114. See Duhigg, supra note 7 (quoting a 2005 email between members of the Google management team, in which one executive wrote that "the real threat if we don't execute on verticals" is "[l]oss of traffic from Google.com because folks search elsewhere for some queries" (internal quotation marks omitted)).

115. See id. ("'We still exist,' says Luther Lowe, a vice president at Yelp, 'but Google did everything it could to ensure that we'd never present a threat to them.'").

116. FTC, Memorandum on Google Inc., File No. 111-0163, at 18–30 (Aug. 8, 2012) [hereinafter FTC Memo]. For the version of the memo as it appeared on the *Wall Street Journal*'s website, see The FTC Report on Google's Business Practices, Wall St. J. (Mar. 24, 2015), http://graphics.wsj.com/google-ftc-report/(on file with the *Columbia Law Review*). The FTC disclosed only the even pages of the staff memo, which represented the views of the Bureau of Competition (BC). Id.

117. FTC Memo, supra note 116, at 30; see also Danny Sullivan, Google Launches "Universal Search" & Blended Results, Search Engine Land (May 16, 2007), https://searchengineland.com/google-20-google-universal-search-11232 [https://perma.cc/6YJ2-HQW2].

118. FTC Memo, supra note 115, at 30.

119. Id. at 24.

120. See id. at 20 (summarizing Google's concern that users would "move[] to vertical search websites," which would, "in turn, become more attractive vehicles for advertisers").

121. Id. at 80.

Google also appropriated information from third-party rivals in order to boost the quality of its own offerings. As of 2012, Google primarily obtained its vertical content through "scraping" other websites.[122] Google did so through pressuring website publishers to accept a license agreement that gave Google blanket consent to use third parties' data feeds.[123] When rivals tried to resist Google's efforts to copy their information, Google gave them an "all-or-nothing choice": They could either allow their content to be appropriated by Google *or* they wouldn't appear within Google web search results at all.[124] In short, Google "could now force local websites—that needed access to Google's web search to reach users—to accede to Google's use of the large storehouse of reviews that Google's rivals had built in order to develop its own user base."[125]

BC staff concluded that the "natural and probable effect" of Google's scraping was "to diminish the incentives of vertical websites to invest in, and to develop, new and innovative content" and recommended that the FTC condemn this conduct as unlawful.[126] BC staff also concluded that Google's self-preferential treatment "likely helped to entrench Google's monopoly power." Although the BC recommended bringing an antitrust action against Google on three grounds,[127] the Commissioners entered a voluntary settlement with the company instead.[128] The European Commission, by contrast, investigated Google on similar grounds and brought two cases establishing that the corporation had abused its dominance.[129]

Given Google's integration across internet search, services, and desktop and mobile advertising markets, there are numerous other ways in which it competes with businesses dependent on its services. In addition to discriminating against vertical content, Google has been found to discriminate against rival horizontal search engines and browsers and to hobble competitors in the search advertising market.[130]

---

122. See id. at 32.

123. Id.

124. Id. at 36.

125. Id.

126. Id. at iii.

127. Id. at 86.

128. Press Release, FTC, Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns in the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search (Jan. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc [https://perma.cc/YPF6-43AV].

129. See Press Release, European Comm'n, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 27, 2017), http://europa.eu/rapid/press-release_IP-17-1784_en.htm [https://perma.cc/K8D6-EL7X] (explaining that Google used its platform to favor its own comparison shopping search engine at the expense of competitors).

130. See Press Release, European Comm'n, Antitrust: Commission Fines Google €1.49 Billion for Abusive Practices in Online Advertising (Mar. 1, 2019), http://europa.eu/rapid/

C. *Facebook*

Facebook is a dominant social network. Around two-thirds of Americans use Facebook, three-quarters of them on a daily basis.[131] In the United States, 80% of user time spent across social networks is spent on Facebook.[132] Through having purchased Instagram and WhatsApp, Facebook now owns the top three, and four of the top eight, social media apps.[133] Like Google, Facebook monetizes its service by selling placement to digital advertisers.[134]

There are at least two sets of market participants that both rely on Facebook's network and find themselves in competition with Facebook: app developers and online publishers. In both markets, Facebook has used its dominant position to appropriate from rivals.

1. *Facebook APIs/Facebook Apps.* — Facebook's network of over two billion users gives app developers an opportunity to reach a large audience.[135] Facebook, meanwhile, has an incentive to cultivate a rich ecosystem of apps built around Facebook's network. To incentivize developers to invest in building this ecosystem, Facebook offers developers access to its application programming interfaces (APIs), which lets apps access data from Facebook's network and grow their number of users.[136] Facebook also delivers certain apps and features directly, placing it in competition with developers. It has both foreclosed competitors from its platform and appropriated their business information and functionality.

Reports describe how Facebook has denied API access to those firms that it considers direct competitors. In 2013, for example, Facebook cut off API access to Vine, the Twitter-owned feature that let users create six-second

---

press-release_IP-19-1770_en.htm [https://perma.cc/BGJ6-LGM5] ("Google has abused its market dominance by imposing a number of restrictive clauses in contracts with third-party websites which prevented Google's rivals from placing their search adverts on these websites.").

131. Aaron Smith & Monica Anderson, Pew Research Ctr., Social Media Use in 2018, at 2 (2018), https://www.pewinternet.org/wp-content/uploads/sites/9/2018/02/PI_2018.03.01_Social-Media_FINAL.pdf [https://perma.cc/J9EP-4TVZ].

132. Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 88 (2019) ("Including time spent on these other platforms, approximately 83% of the consumers' time goes to Facebook and Instagram.").

133. Most Popular Mobile Social Networking Apps in the United States as of October 2018, by Reach, Statista, https://www.statista.com/statistics/579334/most-popular-us-social-networking-apps-ranked-by-reach/ [https://perma.cc/4YDD-82GQ] (last visited Apr. 9, 2019).

134. Facebook, Inc., Annual Report (Form 10-K) 5 (Jan. 31, 2019) [hereinafter 2018 Facebook 10-K], https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm [https://perma.cc/E7PJ-NCMT].

135. Id. at 35.

136. The Graph API, for example, lets developers "read and write to the Facebook social graph." Graph API, Facebook for Developers, https://developers.facebook.com/docs/graph-api/ [https://perma.cc/E4XJ-RXEN] (last visited Apr. 8, 2019).

videos.[137] Emails released by the U.K. Parliament revealed that the decision to block Vine's access came directly from CEO Mark Zuckerberg—presumably because Twitter, which owned Vine, is a Facebook competitor, and Facebook was building out its own video offering.[138] Facebook similarly shut off API access to MessageMe, a messaging app (and competitor to Facebook Messenger) that had soared in popularity, within a week of its release.[139] Voxer, another communications app, was also cut off shortly after Facebook introduced a competing product.[140] Explaining its decision, Facebook cited a provision of its platform policy that prohibited developers from using Facebook APIs to promote a product that replicated "a core Facebook product."[141] The firms that saw their API access revoked by Facebook all ended up either exiting the market or shutting down entirely.[142]

In addition to blocking apps that it deemed competitive threats, Facebook has also systematically copied them. Through Onavo, a mobile-analytics company that Facebook purchased in 2013, Facebook tracked rival apps, identifying which competitors were diverting attention and usage from Facebook.[143] Reports capture how the tool has helped Facebook either imitate rivals or seek to buy them out.[144] Using information captured by Onavo, Facebook has copied the functionality of several apps—including Meerkat,

---

137. Josh Constine, Facebook Is Done Giving Its Precious Social Graph to Competitors, TechCrunch (Jan. 24, 2013), https://techcrunch.com/2013/01/24/my-precious-social-graph/ [https://perma.cc/JQ2J-U3KF].

138. See Note by Damian Collins MP, Chair of the DCMS Committee: Summary of Key Issues from the Six4Three Files and Selected Documents Ordered from Six4Three, Parliament, https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf [https://perma.cc/Y5YC-9A44] (last visited Apr. 10, 2019). The internal documents also reveal that executives kept a "whitelist" of companies that would retain API access. Id.

139. Kim-Mai Cutler, Facebook Brings Down the Hammer Again: Cuts Off MessageMe's Access to Its Social Graph, TechCrunch (Mar. 15, 2013), https://techcrunch.com/2013/03/15/facebook-messageme/ [https://perma.cc/A9CS-U35L].

140. Id. ("The move resembles Facebook's decision last month to shut off Voxer's access to the graph, even though Voxer connected to Facebook for well over a year. . . . Facebook cut the app off around the same time that it launched competing functionality with free voice calling to other users.").

141. Id. In December, a day before Parliament released the Six4Three documents, Facebook ended this policy. Josh Constine, Facebook Ends Platform Policy Banning Apps that Copy Its Features, TechCrunch (Dec. 4, 2018), https://techcrunch.com/2018/12/04/facebook-allows-competitors/ [https://perma.cc/2Q2A-R69Y].

142. See Josh Constine, Facebook Shouldn't Block You from Finding Friends on Competitors, TechCrunch (Apr. 13, 2018), https://techcrunch.com/2018/04/13/free-the-social-graph/facebook-free-the-social-graph/ [https://perma.cc/U8YS-Q839] (observing that Voxer exited the market, MessageMe disintegrated, Vine was shut down, and Phhhoto—a competitor to Instagram that Facebook cut off—closed shop).

143. See Morris & Seetharaman, New Copycats, supra note 10 (describing the internal database that Facebook developed to track rivals through its acquisition of Onavo).

144. See id. (noting that Onavo served as "an internal 'early bird' warning system," flagging potential threats).

Houseparty, and Snapchat—and bought out WhatsApp and tbh.[145] Apps whose functionality Facebook has copied—like Snapchat—went on to see declines in user growth.[146]

Like Amazon and Google, Facebook has established a systemic informational advantage (gleaned from competitors) that it can reap to thwart rivals and strengthen its own position, either through introducing replica products or buying out nascent competitors. Strikingly, one of Facebook's more recent acquisition—the burgeoning social network tbh—had achieved limited market penetration by the time Facebook purchased it.[147] Analysts speculate that Facebook spotted tbh's rapid pace of growth through Onavo and then bought it out.[148]

2. *Facebook's Publishing Network/Facebook Ads.* — For online publishers, Facebook is both a massive communications network on which they've come to depend, as well as a major competitor in selling ad placement. Facebook, meanwhile, has leveraged its dominant position as a communications network to extract sensitive business information from publishers. Collecting this information from publishers has enabled Facebook to significantly enhance the value of its advertising business at publishers' expense.

For publishers, Facebook's network offers a highly attractive distribution channel. Given that most online publishers earn revenue from user clicks and visits, greater exposure to Facebook's 1.52 billion daily users can be a game changer.[149] Citing the promise of greater user visits—and thus greater revenue—Facebook in 2010 started marketing a set of social plug-ins that publishers could add to their websites.[150] Installing the "Like" button, for example, would mean that any user that visited a publisher's website could

---

145. See id; Sarah Perez, Facebook Is Pushing Its Data-Tracking Onavo VPN Within Its Main Mobile App, TechCrunch (Feb. 12, 2018), https://techcrunch.com/2018/02/12/facebook-starts-pushing-its-data-tracking-onavo-vpn-within-its-main-mobile-app/ [https://perma.cc/9GLJ-TF69].

146. See Michelle Castillo, Here Are All the Ways Facebook Has Copied Snapchat, CNBC (Mar. 9, 2017), https://www.cnbc.com/2017/03/09/facebook-copies-snapchat-examples.html [https://perma.cc/8JLT-VA9X] ("[I]t seems the copycat items may be having an effect on Snapchat's slowing user growth rate, even Snap acknowledged Instagram Stories could be a direct competitor in its S-1 filing.").

147. See Josh Constine, Facebook Acquires Anonymous Teen Compliment App tbh, Will Let It Run, TechCrunch (Oct. 16, 2017), https://techcrunch.com/2017/10/16/facebook-acquires-anonymous-teen-compliment-app-tbh-will-let-it-run/ [https://perma.cc/U6RW-RPNW].

148. See Perez, supra note 145.

149. See 2018 Facebook 10-K, supra note 134, at 35.

150. See Facebook for Developers, How to Use the New Facebook Social Plugins for Your Business, Facebook (May 4, 2010), https://www.facebook.com/notes/facebook-for-developers/how-to-use-the-new-facebook-social-plugins-for-your-business/394310302301/ [https://perma.cc/M3ZJ-KBER].

easily share content from the publisher's website with the user's Facebook network, drawing more readers back to the publisher's site.[151]

In order to add Facebook's plug-ins, publishers had to install Facebook's code onto their websites.[152] In practice, installing this code "opened a backdoor communication between users' devices and Facebook's servers," enabling Facebook to leverage the social plug-ins installed on third-party websites to track the users of those websites.[153] In other words, Like buttons dramatically expanded the reach of Facebook's tracking: Any time a Facebook user visited a site with the social plug-in, Facebook could use the user's Facebook login cookies to identify the user.[154] Some publishers were wary. The value that online publishers offer advertisers is access to their specific readers; it is this audience relationship that ultimately allows ad-based publishers to monetize their content. If Facebook were able to surveil a publisher's readers, it could sell access to those readers at a fraction of the publisher's price—undercutting the publisher's pricing power in the ad market.[155] For Facebook, meanwhile, access to this data would enable it to more precisely target Facebook users when selling ads, increasing ad revenue.

To assuage publishers' concerns, Facebook maintained the perception that it would not use these plug-ins to monitor users for the purpose of selling advertising.[156] Keen to harness Facebook's expansive network to increase clicks, publishers flocked to the plug-ins. Within the first week of the rollout, over 50,000 websites installed Facebook's social plug-ins,[157] helping Facebook embed its code across the internet.[158] Contrary to Facebook's representations, researchers later exposed that Facebook was using the Like button code to track what users were reading or buying—even if a user hadn't clicked the Like button and even if the user had logged out of Facebook.[159] Despite facing public backlash for both its apparent deception and its pervasive surveillance, Facebook did not change course—perhaps because it no longer faced serious competition in the social network market.[160] In 2014, it officially codified its policy of using

151. As Facebook described, "When a person clicks Like, it (1) publishes a story to their friends with a link back to your site, (2) adds the article to the reader's profile, and (3) makes the article discoverable through search on Facebook." See Facebook Media, The Value of a Liker, Facebook (Sept. 29, 2010), https://www.facebook.com/notes/facebook-media/value-of-a-liker/150630338305797 [https://perma.cc/D2RR-3LSX].

152. Srinivasan, supra note 132, at 63.

153. Id. at 63–64.

154. Id. at 65.

155. Id. at 64.

156. Id. at 64 ("For many years, Facebook perpetuated the belief it would not leverage backdoor access, the way it had with Beacon, to conduct surveillance for commercial purposes.").

157. Facebook for Developers, supra note 150.

158. Srinivasan, supra note 132, at 64.

159. Id. at 65–66.

160. Id. at 66–69.

Facebook code embedded across third-party websites to track users.[161] The new policy admitted that Facebook would now use this surveillance data to boost Facebook's advertising business.[162]

It is reasonable to consider this policy change a bait and switch. Facebook induced websites to install Facebook plug-ins by representing that the company would not use this installed code to channel user data to its advertising business. Thirty percent of the top million most-visited websites—including major news publishers—added Facebook's plug-ins, becoming dependent on Facebook's network for greater distribution.[163] Facebook's decision to switch course has meant that online publishers—and any third-party website that both sells ads and uses Facebook plug-ins—are now feeding valuable business data to a major competitor at their own expense.

Unlike the case of Amazon or Google, Facebook's appropriation of publishers' business information is not a feature of Facebook being vertically integrated. Instead, it derives from the fact that Facebook is both a major communications network and a major advertiser, and the price it charges publishers for using its platform as a distribution network is the right to surveil publishers' users—information that it uses to enrich its advertising business. In other words, collecting publishers' business information is not a functional necessity of allowing publishers to use Facebook; it is instead the condition Facebook has set.

There are aspects of Facebook's business in which it is integrated, such as in content. Through Facebook Instant Articles, for example, Facebook has vertically integrated into publishing media content on its own platform.[164] Reports suggest that Facebook has used its integrated structure to preference its own offerings.[165]

D. *Apple*

Apple is a major provider of consumer electronics and digital services, spanning smartphone and smartwatch devices, desktop and laptop computers, digital assistants, a music store, and set-top boxes. The first publicly traded

---

161. Id. at 70 ("In June of 2014, Facebook announced it would leverage its code presence on third-party applications to track consumers, enabling it to surveil the specific online behavior of this country's citizens despite widespread preference to the contrary.").

162. Id. at 71 ("But now Facebook changed course and announced that the data derived from tracking consumers would augment Facebook ad targeting, attribution, and measurement.").

163. Steven Englehardt & Arvind Narayanan, Online Tracking: A 1-Million-Site Measurement and Analysis, 2016 Proc. ACM SIGSAC Conf. on Computer & Comm. Security 1388, 1395 fig.2.

164. Facebook: By Prioritizing Natively Published Articles in Its News Feed, Facebook Risks Antitrust Enforcement, Cuts Off Traffic and Data to Publishers, The Capitol Forum (Nov. 14, 2016), https://thecapitolforum.com/wp-content/uploads/2016/07/Facebook-2016.11.04.pdf (on file with the *Columbia Law Review*).

165. See id. ("Facebook pulls a number of levers to keep users on its own platform rather than going to the websites of publishers who fuel Facebook with free content. Such tactics mirror conduct that has landed Google in antitrust trouble in Europe.").

corporation in history to reach $1 trillion valuation,[166] Apple is a major provider of mobile devices and operating systems in the United States.[167]

Across its products, Apple has long championed a vertically integrated model that combines hardware, software, services, and retail.[168] Unlike the Android operating system—which users operate on non-Alphabet devices—Apple iOS functions only on Apple devices.[169] Like Android, Apple both operates an app marketplace, offering third-party app developers the opportunity to reach Apple customers, and directly markets its own apps in its app marketplace.[170] Since it opened in 2008, the App Store has generated more than $120 billion in total sales for app developers.[171]

1. *Apple iOS/App Store/Apple Apps.* — App developers claim that Apple uses its integrated model to privilege its own apps by setting unfavorable terms for third parties.[172] A recent complaint filed by Spotify in the European Union

166. Thomas Heath, Apple Is the First $1 Trillion Company in History, Wash. Post (Aug. 2, 2018), https://www.washingtonpost.com/business/economy/apple-is-the-first-1-trillion-company-in-history/2018/08/02/ea3e7a02-9599-11e8-a679-b09212fb69c2_story.html (on file with the *Columbia Law Review*).

167. Mobile Operating System Market Share in United States of America, StatCounter, http://gs.statcounter.com/os-market-share/mobile/united-states-of-america [https://perma.cc/VT92-JE9M] (last updated Mar. 2019) (documenting that, as of March 2019, iOS captured 55% of the mobile operating system market); US Smartphone Market Share: By Quarter, Counterpoint (Feb. 19, 2019), https://www.counterpointresearch.com/us-market-smartphone-share/ [https://perma.cc/Y7KT-3A2C] (documenting that, at the end of 2018, Apple captured 47% of the U.S. smartphone market).

168. Apple has been designing more and more of the technologies inside its products, including chips. Mark Gurman, How Apple Built a Chip Powerhouse to Threaten Qualcomm and Intel, Bloomberg (Jan. 29, 2018), https://www.bloomberg.com/graphics/2018-apple-custom-chips/ (on file with the *Columbia Law Review*). In the last couple of years, however, Apple has broken from its original model by been making Apple services available on non-Apple devices. See Michael Simon, Apple Will Launch iTunes Video App on Samsung Smart TVs This Spring—and It'll Support Bixby, Macworld (Jan. 6, 2019), https://www.macworld.com/article/3331183/itunes-app-samsung-smart-tv.html [https://perma.cc/K7XU-4MHS] (noting that Apple is placing a TV app on hardware produced by Samsung and is placing Apple Music on smart speakers produced by Amazon).

169. See iOS 11 Is Compatible with These Devices, Apple, https://support.apple.com/en-us/HT209574 [https://perma.cc/P6BR-4TG8] (last visited Apr. 2, 2019).

170. See Stephen Silver, The Revolution Steve Jobs Resisted: Apple's App Store Marks 10 Years of Third-Party Innovation, Apple Inside (July 10, 2018), https://appleinsider.com/articles/18/07/10/the-revolution-steve-jobs-resisted-apples-app-store-marks-10-years-of-third-party-innovation [https://perma.cc/FG8G-VDMC].

171. Tripp Mickle, With iPhone Sputtering, Apple Bets Future on TV and News, Wall St. J. (Mar. 25, 2019), https://www.wsj.com/articles/with-the-iphone-sputtering-apple-bets-its-future-on-tv-and-news-11553437018 (on file with the *Columbia Law Review*).

172. Few developers have publicly reported discrimination by Apple, so this section will necessarily focus on and draw from Spotify, which recently filed a complaint in the European Commission, claiming that Apple has engaged in anticompetitive conduct by abusing its control over the App store. For Spotify's summary of its claims against Apple, see The Case, Time to Play Fair, https://timetoplayfair.com/the-case/ [https://perma.cc/

summarizes these allegations.[173] First, Apple charges Spotify and certain other apps a 30% fee on in-app purchases—a fee that, Spotify points out, Apple enforces selectively.[174] Apple's own apps do not pay the fee, and neither do many apps, like Uber, that are not in direct competition with a comparable Apple service.[175] Second, Apple prevents Spotify from communicating directly with Apple-based users or marketing certain services to them—potentially inhibiting Spotify's sales.[176] And third, Spotify alleges that Apple "routinely reject[ed]" Spotify's app enhancements and bug fixes—degrading the product quality it could market through Apple, as Apple ramped up its competitor service, Apple Music.[177]

This is not the first time that developers have alleged discrimination by Apple. Around 2008, Apple explicitly rejected apps on the basis that they "duplicate[d] the functionality" of built-in iPhone apps.[178] More recently, Apple was reported to have removed a digital wellness app shortly after releasing its own rival product (Screen Time)[179] and to have rejected a social location planning app that competes with its own "Find My Friends" app.[180]

Faced with slowdown of iPhone sales, Apple is expanding its service offerings, introducing new services in TV, news, payments, and video games.[181] It has also "intensified monitoring of apps that benefit and threaten Apple," in part by creating a "release radar" through which Apple tracks apps that pose

444C-BPFV] [hereinafter Spotify Case] (last visited Apr. 1, 2019). For Apple's response to Spotify's claims, see Addressing Spotify's Claims, Apple (Mar. 14, 2019), https://www.apple.com/newsroom/2019/03/addressing-spotifys-claims/ [https://perma.cc/85YP-T7LD] [hereinafter Apple Response].

173. See Spotify Case, supra note 172 (claiming that "Apple's actions violate the law" by selectively discriminating against competitors on the Apple platform); see also Joan E. Solsman, Spotify: Apple's App Store Abuses Its Power to 'Stifle' Rivals, CNET (Mar. 14, 2019), https://www.cnet.com/news/spotify-apple-app-store-abuses-power-to-stifle-competition/ (on file with the *Columbia Law Review*) (paraphrasing Spotify CEO David Ek of saying that "Apple wields its powerful App Store as a cudgel to stifle innovation, weaken competition and unfairly tax its rivals").

174. Five Fast Facts, Time to Play Fair, https://timetoplayfair.com/facts/ [https://perma.cc/37VV-JMTW] [hereinafter Spotify Facts] (last visited Apr. 2, 2019).

175. Id. In its response, Apple noted that in-app fees are the only source of revenue for the Apple app store. See Apple Response, supra note 172.

176. Spotify Facts, supra note 174.

177. Id.

178. Chris Foresman, Apple Rejects Another App for "Duplicating Functionality," Ars Technica (Sept. 22, 2008), https://arstechnica.com/gadgets/2008/09/apple-rejects-another-app-for-duplicating-functionality/ [https://perma.cc/2Y8G-UETK] (internal quotation marks omitted) (quoting Apple).

179. Mark Wolgemuth, RescueTime for iOS Update: Apple Has Removed Us from the App Store, RescueTime: Blog (Nov. 8, 2018), https://blog.rescuetime.com/rescuetime-for-ios-removed/ [https://perma.cc/KJQ2-JF78].

180. See Michael McClain, Apple Rejecting "Find My Location" Competitor Apps?, Medium (Aug. 13, 2018), https://medium.com/@michael.c.mcclain/apple-rejecting-find-my-location-competitor-apps-68c12b4c4aae [https://perma.cc/9JNK-8MNQ].

181. See Mickle, supra note 171.

competitive threats to Apple's own services.[182] It is unclear whether Apple's monitoring efforts are drawing on data on rivals collected through its platform.

E. *Effects of Discrimination and Appropriation on Investment and Innovation*

There are several reasons why permitting dominant digital platforms to discriminate against and appropriate sensitive business information from producers that depend on them to reach market might be harmful. Drawing on a Progressive Era framework, one could argue that allowing a firm that controls an essential service or form of infrastructure to exploit that control in ways that enrich the firm and harm third-party dependents amounts to a problematic exercise of private coercion.[183] Seen through this lens, this conduct represents the accumulation of "arbitrary authority unchecked by the ordinary mechanisms of political accountability," amounting to a "political problem of domination."[184]

As Part II of this Article traces, in recent decades this expansive framework for understanding and regulating private power has been abandoned in favor of a paradigm that focuses primarily on welfare costs. Yet, as this section outlines, platform discrimination and appropriation also risk undermining innovation, raising dynamic efficiency concerns. Therefore, even under a framework primarily focused on efficiency harms, discrimination and appropriation by dominant platforms merits serious concern.

1. *Are Dominant Digital Platforms Stifling Innovation?* — One risk associated with foreclosure and value appropriation by dominant digital platforms is that this conduct could deter entry and chill innovation. If independent developers or producers rely on a dominant platform to reach customers and also face the constant risk that the platform will foreclose access, appropriate their business value, or both, producers may be less likely to secure funding and develop their product in the first place. In *Microsoft*, the district court found that Microsoft's exclusionary conduct not only had hobbled innovation in middleware and applications software but had discouraged competition throughout the computer industry as a whole.[185] The long-term effect of its conduct was to "deter[] investment in technologies and businesses that exhibit[ed] the potential to threaten Microsoft."[186]

Anecdotal evidence suggests that both actual entry and the threat of entry by digital platforms into platform-adjacent markets is dampening investment in

---

182. Id.

183. See Rahman, New Utilities, supra note 26, at 1628 ("The challenge for law and public policy, then, was not just to promote economic efficiency and well-functioning markets. Rather, the challenge was a broader *political* one, of ensuring the accountability of private actors to the public good . . . .").

184. Id. at 1629.

185. See United States v. Microsoft Corp., 65 F. Supp. 2d 1, 103 (D.D.C. 1999) ("Most harmful of all is the message that Microsoft's actions have conveyed to every enterprise with the potential to innovate in the computer industry.").

186. Id.

complementary segments, now known as a "kill-zone."[187] For example, a survey of more than two dozen Silicon Valley investors revealed that Facebook's willingness to appropriate information from and mimic the functionality of apps has created "a strong disincentive for investors" to fund services that Facebook might copy.[188] One founder observed, "People are not getting funded because Amazon might one day compete with them."[189] "We don't touch anything that comes too close to Facebook, Google or Amazon," said a managing partner at New Enterprise Associates.[190] Another venture capital investor noted that the impact of dominant digital platforms on "what can be funded, and what can succeed, is massive."[191] This concern raised by venture capitalists makes sense: A potential innovator (or a potential funder of a potential innovator) decides whether to invest based on the anticipated risk and reward of realizing the innovation. Anticipating platform discrimination or appropriation will lower expected rewards, depressing the incentive to invest. Even the uncertainty of discrimination can dissuade entry by heightening risk.

Data on investment trends do not offer a decisive answer but generally seem consistent with the story told by surveyed investors. Venture capital funding as a whole appears to be booming: In 2018, the total annual venture capital invested surpassed $100 billion for the first time since the dot-com period.[192] The number of angel and seed investments, meanwhile, has been declining since 2015, signaling that it has become harder for startups to secure an initial round of financing.[193] Indeed, it is late-stage deals with mature

187. See American Tech Giants Are Making Life Tough for Startups, Economist (June 2, 2018), https://www.economist.com/business/2018/06/02/american-tech-giants-are-making-life-tough-for-startups (on file with the *Columbia Law Review*).

188. Dwoskin, supra note 10. For a counterperspective, see Oliver Wyman, Assessing the Impact of Big Tech on Venture Investment 5 (2018), https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/july/assessing-impact.pdf [https://perma.cc/9CM8-CC9T] (concluding that there has been "no negative impact of [Facebook, Google, and Amazon] presence on venture capital deal value"). The report was commissioned by Facebook. Id. at 1. For a useful critique of the Wyman study, see Ian Hathaway, Platform Giants and Venture-Backed Startups (Oct. 12, 2018), http://www.ianhathaway.org/blog/2018/10/12/platform-giants-and-venture-backed-startups [https://perma.cc/SZ8U-QLKS] (arguing that the category fields used by Wyman are too broad to be meaningful).

189. Solon, supra note 11 (internal quotation marks omitted).

190. Dwoskin, supra note 10 (internal quotation marks omitted).

191. Schechter, supra note 11. One can imagine investors holding back from funding services that strive to go head-to-head with a digital platform in its primary market, *or* from withholding funding from services that seek to operate in a complementary market. These quotations are not entirely clear as to which of the two is occurring.

192. PitchBook Data, Inc. et al., Venture Monitor: 4Q 2018, at 4 (2018), https://files.pitchbook.com/website/files/pdf/4Q_2018_PitchBook_NVCA_Venture_Monitor.pdf [https://perma.cc/Q9FE-NYHM] ("The 2018 VC headline is, understandably, that annual capital invested eclipsed $100 billion for the first time since the dot-com era."). Investors note that the current abundance of capital at least partly reflects "investor demand for growth assets during a time of historically low interest rates." Id. at 14.

193. See id. at 8. Although the total deal value for angel- and seed-stage deals in 2018 approached a decade high, the relatively strong activity helped "stymie a downward trend." Id.

companies that account for an "outsized proportion" of total capital today,[194] while startups see fewer first financings, even as the deal value for startups has increased.[195] In other words, venture capital markets seem to be following a winner-take-most model: Fewer firms receive funding, but those that do are raising more capital.[196] These trends come against a backdrop of falling entrepreneurship: Startup formation is at a thirty-year low, contributing to a loss of business dynamism.[197]

These overall numbers, however, offer limited insight into whether—and in what way—dominant platforms are affecting venture capital funding. Even sector-specific figures compiled by the industry database are based on industry classifications that are too generalized for a precise analysis of this question. Establishing high-level causality between platform conduct and investment decisions would prove extremely challenging; there are a significant number of variables at play, and demonstrating but-for causality is tough. Achieving clarity on this question would require granular case-by-case analysis.[198]

The theoretical literature examining how third-party producers and providers (also called "complementors") manage or respond to head-to-head competition with platforms is vast.[199] Empirical work, by contrast, is more limited.

One study found that Amazon is more likely to enter product spaces that have higher sales, better reviews, and that do not require significant effort by sellers to grow.[200] The effect of Amazon's entry, meanwhile, is to reduce shipping costs for consumers and increase sales—but its self-preferential treatment can also foreclose consumers' access to competing products.[201] Overall, Amazon's entry has not yet affected customer perceptions of product

194. Id. at 5.

195. See id. at 10.

196. Id. ("Startups see fewer, but larger first financings[.]").

197. See Ryan A. Decker et al., Declining Business Dynamism: What We Know and the Way Forward, 106 Am. Econ. Rev. (Papers & Proc.) 203, 203 (2016); see also Germán Gutiérrez & Thomas Philippon, Declining Competition and Investment in the U.S. 1 (Nat'l Bureau of Econ. Research, Working Paper No. 23,583, 2017) ("[T]here has been a broad decrease in turnover and a broad increase in concentration across most U.S. industries.").

198. See Hathaway, supra note 188.

199. For literature that identifies this entry strategy as enabling a platform to strengthen its market power, see, for example, Dennis W. Carlton & Michael Waldman, The Strategic Use of Tying to Preserve and Create Market Power in Evolving Industries, 33 RAND J. Econ. 194, 194 (2002); Michael D. Whinston, Tying, Foreclosure, and Exclusion, 80 Am. Econ. Rev. 837, 850–56 (1990). For literature that focuses on how this strategy can discourage third parties from innovating, see, for example, Joseph Farrell & Michael L. Katz, Innovation, Rent Extraction, and Integration in Systems Markets, 48 J. Indus. Econ. 413, 414 (2000) ("[I]ntegration can inefficiently reduce incentives to innovate when consumers differ in their valuations of the innovation."). See also infra Appendix.

200. See Zhu & Liu, supra note 33, at 2620.

201. Id. at 2632.

quality,[202] but it does "discourage[] third-party sellers from continuing to offer the products."[203] The authors of that study note that existing merchants discouraged by Amazon's entry "may bring fewer innovative products to the platform."[204]

A study assessing how app developers reacted to perceived or actual entry by Google, meanwhile, found that developers are "discouraged from innovating in the affected market."[205] Indeed, even the *threat* of direct competition by Google spurs developers to "significantly reduce[]" updates on affected apps—and to reallocate their efforts to markets unaffected by Google's entry.[206] Notably, the average small firm also responds by pivoting to a focus on short-term profits, leading to higher prices.[207]

Empirical studies assessing how actual or potential entry by a dominant platform affects complementors are still limited. Investors acknowledge unequivocally that the dominance of digital platforms deters investment in certain markets, and data suggest that firms looking to compete with a core functionality of Google, Facebook, or Amazon have seen funding dry up.[208] The few available case studies confirm that the risk of appropriation chills or at

---

202. Id. ("[W]e do not find differences between the average product ratings of affected and unaffected products, suggesting that Amazon's entry does not seem to increase consumer satisfaction with the products.").

203. Id.

204. Id. at 2638. Although Amazon's conduct deters entry, Professors Feng Zhu and Qihong Liu speculate that there could be a countervailing effect. Insofar as Amazon's lower prices could expand its consumer base, this could in theory spur new merchants to join Amazon. Id. ("How Amazon's direct competition against its complementors affects platform growth thus remains an open question."); see also Feng Zhu, Friends or Foes? Examining Platform Owners' Entry into Complementors' Spaces, 28 J. Econ. & Mgmt. Strategy 23, 26 (2019) ("[I]f Amazon's entries attract more consumers, the expanded customer base could incentivize more third-party sellers to join the platform. As a result, the long-term effects for consumers of Amazon's entry are not clear.").

205. Wen Wen & Feng Zhu, Threat of Platform-Owner Entry and Complementor Responses: Evidence from the Mobile App Market 16 (NET Inst., Working Paper No. 16-10, 2018). Specifically, the study found that when a developer is faced with the threat of Google's entry, the developer "significantly reduces its updates on the affected app by 5 percent relative to an unaffected developer's app," while *actual* entry by Google leads the developer to reduce updates on the affected app by eight percent. Id. Notably, Google's threat of entering a particular app market drives the affected developer to "significantly increase[]" updates on unaffected apps. Id.

206. Id. Notably, Google's threat of entering a particular app market drives the affected developer to "significantly increase" updates on unaffected apps. Id. The authors conclude that "[o]verall, these figures suggest that after Google becomes a credible threat in certain markets, developers become less interested in offering new products in those markets." Id. at 23.

207. Id. at 5 ("Further, in contrast to other studies that find that entry threat reduces prices, we show that the average small firm increases prices because, faced with the entry threat of a powerful firm, it may decide to focus on short-term profits."). The finding that platform entry redirects innovation rather than stifles it altogether could be seen as reducing "product redundancy" and "wasteful effort." But one cost to this approach is that it risks replacing the competitive process with Google as the arbiter of what products fail or survive. Id. at 26.

208. See Hathaway, supra note 188 ("[T]he expansion of venture capital first financings grew more slowly or contracted more rapidly in each detailed FGA industry than it did for comparable sub-sectors (Software, Retail), sectors (IT, B2C), and for the rest of venture capital as a whole.").

least diverts certain forms of investment and innovation. More empirical work on this issue would help deepen public understanding of how funders assess the risk of platform foreclosure and appropriation, and what impact platform expansion into adjacent markets may have on innovation.

At first glance, the idea that dominant digital platforms may be using their integrated structure to undermine dynamic efficiency appears in tension with standard economic theory. The Appendix to this Article reviews leading theories on when integrated firms can be expected to discriminate against or exclude rivals in adjacent markets, identifies the set of conditions under which this is likely to happen, and explains why digital platform markets fit these conditions.

2. *Innovation and Platform Design Principles.* — While initial evidence suggests that platform discrimination and appropriation is stifling innovation, definitively determining the net effects on innovation—which involves significant uncertainty, lengthy time horizons, and interdependencies[209]—is complex. Indeed, the debate over what type of market structure and forms of business organization best promote innovation is longstanding and extensive.[210] While contributing to this debate is beyond the scope of this Article, this section will briefly offer that (1) promoting innovation in platform-adjacent markets should be a key goal of platform policy, and (2) innovation architecture literature offers useful principles for thinking through how to create digital platform ecosystems conducive to innovation.

There is broad consensus that, over the long run, promoting dynamic efficiency is more important to well-being than static efficiency.[211] For this reason, scholars have devoted a wealth of research to identifying how to

---

209. See Melissa A. Schilling, Towards Dynamic Efficiency: Innovation and Its Implications for Antitrust, 60 Antitrust Bull. 191, 199 (2015).

210. The rich and complex literature on this topic is often described in shorthand as a debate between Kenneth Arrow and Joseph Schumpeter. See, e.g., Jonathan B. Baker, Beyond Schumpeter vs. Arrow: How Antitrust Fosters Innovation, 74 Antitrust L.J. 575, 575 (2007) (describing the debate over the best way to foster innovation as pitting the view of Arrow against that of Schumpeter). At the risk of oversimplification, Arrow argued that competition spurs innovation, while Schumpeter argued that oligopolistic markets do. Compare Kenneth J. Arrow, Economic Welfare and the Allocation of Resources to Invention, *in* The Rate and Direction of Inventive Activity: Economic and Social Factors 609, 620 (Nat'l Bureau of Econ. Research ed., 1962) ("The preinvention monopoly power acts as a strong disincentive to further innovation."), with Joseph A. Schumpeter, Capitalism, Socialism, and Democracy 106 (1942) ("The firm of the type that is compatible with perfect competition is in many cases inferior in internal, especially technological, efficiency."). For a high-level review of this debate, see generally Carl Shapiro, Competition and Innovation: Did Arrow Hit the Bull's Eye?, *in* The Rate and Direction of Inventive Activity Revisited (Josh Lerner & Scott Stern eds., 2012). See also Mark A. Lemley, Industry-Specific Antitrust Policy for Innovation, 2011 Colum. Bus. L. Rev. 637, 651–52 (arguing that the "relationship between market structure and innovation is industry-specific" and demanding a more industry-specific innovation policy).

211. Herbert Hovenkamp, Antitrust and Innovation: Where We Are and Where We Should Be Going, 77 Antitrust L.J. 749, 751 (2011) ("[T]here seems to be broad consensus that the gains to be had from innovation are larger than the gains from simple production and trading under constant technology.").

cultivate and promote instrumentalities of innovation.[212] Commonly recognized innovation catalysts include patents, standard-setting processes, and platforms.[213]

Because platforms have the potential to lower the cost of entry for firms looking to market new products or services, platforms have the potential to "increase the rate at which product innovation can happen."[214] The Windows platform had the potential to ease entry for Netscape, which could access millions of consumers without having to create its own operating system—just as Android has the potential to ease entry for thousands of app developers. Given the critical role that platforms can play in spurring innovation, protecting the integrity of platforms as innovation catalysts should be a key goal of competition policy in digital markets.[215] This would include preventing platforms from engaging in forms of discrimination, exclusion, appropriation, and self-privileging, conduct that can lead to "the corruption of the entire system of platform-based innovation."[216]

Separate from policing conduct that risks undermining innovation, policy can also draw from innovation architecture principles.[217] This approach was central to designing the internet, whose original architecture was based on the "end-to-end" principle.[218] In general, end-to-end stipulates that "the

212. See generally Innovation Clusters and Interregional Competition (Johannes Bröcker, Dirk Dohse & Rüdiger Soltwedel eds., 2003) (collecting essays that discuss how the spatial clustering of firms impacts regional productivity and innovation levels); Innovation Networks and Clusters: The Knowledge Backbone (Blandine Laperche, Paul Sommers & Dimitri Uzunidis eds., 2010) (collecting essays that explain how promoting collaboration and networks among firms, which can be used to share knowledge about innovation, can produce new and useful forms of knowledge); Steven Johnson, Where Good Ideas Come From: The Natural History of Innovation (2010) (discussing and analyzing the environments and conditions that are most conducive to innovation and identifying seven factors that are most likely to lead to innovation in any context).

213. Tim Wu, Taking Innovation Seriously: Antitrust Enforcement if Innovation Mattered Most, 78 Antitrust L.J. 313, 321 (2012) [hereinafter Wu, Taking Innovation Seriously] ("[T]here are some instrumentalities that do lie within the domain of competition enforcement. Here I want to focus on three: Standard Setting, Platforms, and Patents.").

214. Id.

215. Id. at 322 ("Given the importance of platforms and standard setting to innovation, an innovation-centered law would make a major goal the protection of the integrity of these instrumentalities.").

216. Id. at 323; see also id. at 324 (noting that, were antitrust enforcement purely innovation-focused, "the treatment of applications by platform owners would be the subject of continuing oversight.").

217. Barbara van Schewick, Internet Architecture and Innovation 4 (2010) [hereinafter van Schewick, Internet Architecture] ("Different architectures may impose different constraints, which may result in different decisions by economic actors, which in turn may result in different firm and market structures and different levels of economic activity.").

218. Lemley & Lessig, supra note 16, at 931 (describing the end-to-end principle as a fundamental design feature of the Internet). As Professor Barbara van Schewick notes, there is a "broad" and "narrow" version of the end-to-end principle. Van Schewick, Internet Architecture, supra note 217, at 37–38 ("As will become apparent, some of the confusion can be attributed to the silent coexistence of two different design principles under the same name: the narrow version and the broad version of the end-to-end arguments."); id. at 60–79 (contrasting the two versions).

'intelligence' in a network should be located at the top of a layered system—at its 'ends,' where users put information and applications onto the network[,]" while the "communications protocols themselves (the 'pipes' through which information flows) should be as simple and as general as possible."[219] Professors Mark Lemley and Lawrence Lessig observe that designing the Internet around end-to-end has had social significance, most notably in "the competition in innovation the Internet enables."[220] As they explain, because "there is no single strategic actor who can tilt the competitive environment (the network) in favor of itself, or no hierarchical entity that can favor some applications over others, an e2e network creates a maximally competitive environment for innovation."[221]

The end-to-end principle was embedded partly through the Internet Protocol, an open-standard networking protocol that empowered "developers at the network's edge to design and deploy new services and applications without having to rely on network operators to build any new functionality into the physical core of the network."[222] This principle, in turn, traces to the concept of common carriage, which required common carriers to grant equal treatment to equally situated parties.[223] The key attributes of common carriage are "nondiscriminatory public access and indifference to the nature of the goods carried."[224]

Digital platforms exist in a different "layer" from the physical network providers governed by end-to-end.[225] As scholars have noted, regulations at the "application" layer—which includes digital platforms—have encouraged "content awareness," in part due to the role some of these services play in intermediating speech and expression.[226] Still, these architecture design principles offer a fruitful way of thinking through what set of constraints should apply to dominant digital platforms in order to best promote innovation.

II. LEGAL SCRUTINY OF VERTICAL INTEGRATION BY DOMINANT NETWORKS

Confronting the risks of integration by dominant intermediaries is not new. Up until around the 1970s, a basic regulatory principle held that dominant

---

219. Lemley & Lessig, supra note 16, at 930–31.

220. Id. at 930.

221. Id. at 931.

222. Annemarie Bridy, Remediating Social Media: A Layer-Conscious Approach, 24 B.U. J. Sci. & Tech. L. 193, 200–01 (2018) ("IP is the open-standard networking protocol that allows heterogeneously configured local area networks from all over the world to interconnect with one another.").

223. See id. at 201.

224. Id.

225. Kevin Werbach, A Layered Model for Internet Policy, 1 J. on Telecomm. & High Tech. L. 37, 59 (2002) (distinguishing between four layers that comprise the Internet: physical, logical, applications or services, and content).

226. Bridy, supra note 222, at 205; see also Brett M. Frischmann, Infrastructure: The Social Value of Shared Resources 319–23 (2012) (describing a five-layer model of internet infrastructure).

gatekeepers should not be permitted to compete with third parties for access to the gatekeeper's facilities. Limits on business entry for network monopolies, gatekeeper intermediaries, and other businesses deemed to have outsized control over key services were a mainstay of economic regulation.

This Part traces the evolution in both the institutional mechanisms and the substantive considerations by which government actors have imposed limits on business entry. It closes by sketching out how current antitrust law neglects to address harms from vertical integration that should trigger scrutiny even under the current framework.

Notably, state and federal governments have issued line-of-business restrictions through a variety of legal tools: corporate charters, regulatory regimes, and antitrust law.[227] In some cases, these limits prohibited firms from expanding into *any* distinct market; in others, they prohibited firms from entering only *adjacent* markets—namely, those markets that involve a successive stage of production or distribution. A categorical prohibition would, for example, ban a movie distributor from entering any nondistributor market, whereas a ban on integration would prohibit it from entering only the movie-production market or the movie-theater market. Since this Article examines the dual role that digital platforms play—as both marketplace operators and merchants in the marketplace—this Part primarily focuses on limits on entry into adjacent markets.

A. *Evolving Approaches to Restricting Business Lines*

Early American corporations had their activities restricted by their charters. States issued corporate charters as a special grant of limited liability in exchange for the performance of specific duties and functions.[228] Corporate charters generally limited the size, scope, and duration of operations and steered business activity toward serving community purposes.[229] This effort to use charters to impose "some degree of social control" on firms lasted into the late nineteenth century, by which point most state legislatures had passed general incorporation laws—with the expectation that companies would now

---

227. See infra section II.A.

228. This notion of the corporate form stemmed from early English law, where corporations were

> in form, in fact, and in legal cognizance a device by which the political state got something done. They were far more like the bodies corporate we call 'public authorities' today . . . . Few in the seventeenth or eighteenth centuries would have disputed that a corporation was an agency of the state—probably not before the early nineteenth century, either in England or in the United States.

Adolf A. Berle, Jr., Constitutional Limitations on Corporate Activity—Protection of Personal Rights from Invasion Through Economic Power, 100 U. Pa. L. Rev. 933, 944 (1952).

229. Id. at 935 (describing "attempts to limit by charter the size or the scope of operations, or to guide into, or hold operations in, some specific field of activity, . . . or [to] direct[] corporate action for community purposes," which carried forward into nineteenth-century state incorporation statutes but were then abandoned).

be regulated by competition.[230] With this shift from special to general incorporation, the corporation largely ceased being viewed as an instrument of state policy and instead became seen as a "private institution" that had authority "to carry on virtually any kind of business."[231]

Following this shift, restricting the lines of business in which a firm could engage mostly fell to regulatory regimes that Congress introduced to govern specific sectors. Typically overseen by an administrative agency, these regulatory regimes spanned industries including railroads, banking, airlines, trucks, telecommunications, electricity, and natural gas—sectors considered both critical to the economy and, in some cases, susceptible to monopolistic market structures.[232] In some instances, the statute creating the regulatory regime specifically prohibited regulated firms from entering certain markets.[233] In other cases, these limits on entry (and exit) were instituted by the administrative agency.[234]

While each regime had its own specific policy goals and regulatory tools, government oversight of these "regulated industries" shared a general aim of ensuring reliability and nondiscrimination.[235] Agencies applied restrictions on market entry and exit to promote both of these goals.[236] In some cases, regulated firms were permitted to enter multiple markets so that they could cross-subsidize: Long-distance service, for example, could subsidize local service, enabling the provision of universal service.[237] In other instances, regulated firms were prohibited from entering certain lines of business in order to further the goal of nondiscrimination.[238] While common carriage regimes would require a firm to offer equal service on equal terms, prohibiting a firm from competing with its business customers would eliminate one source of the incentive to discriminate. In this way, common carriage and structural separations often functioned as complements in the service of nondiscrimination. In addition to limiting entry and exit, standard agency interventions

230. Id. at 935, 946.

231. Id. at 946. Of course, this view of corporations as private actors did not override the recognition that the corporate form derived its legal protections from the state. Indeed, "[c]ourts continued to insist that ultimate control over and responsibility for the administration and functioning of the corporation remained with the state because the corporation's existence and functioning was an exercise of the sovereign political power of the state itself." Id.

232. See Joseph D. Kearney & Thomas W. Merrill, The Great Transformation of Regulated Industries Law, 98 Colum. L. Rev. 1323, 1325–27 (1998).

233. See infra sections III.A–.B.

234. See infra sections III.C–.D.

235. Kearney & Merrill, supra note 232, at 1325.

236. See id. at 1359 ("[T]he regulatory agency would make the initial and central determination of whether companies would be permitted to enter the industry.").

237. Id. at 1340.

238. See id. at 1359.

included regulating rates, requiring standard packages of services at uniform prices, and mandating universal service.[239]

No precise set of criteria determined the sectors that Congress decided to oversee through regulatory regimes. Several of the regulated industries exhibited natural monopoly characteristics—including high fixed costs and low marginal costs—but these economic characteristics offer only a partial explanation.[240] Direct government oversight tended to hinge more on the degree to which an industry was, as the Supreme Court termed it, "affected with a public interest."[241] In some cases, the "public-ness" of an industry correlated to the degree to which it was a public necessity, as was the case, for example, with electricity.[242] Nondiscriminatory access requirements, however, were generally tied to physical distribution networks, which the government has a long history of overseeing.[243] All regulated industries were related in some way to transportation and communication networks, even as "different economic and social facts seem to carry different weight" depending on the context.[244]

As Professors Joseph Kearney and Thomas Merrill have described, starting in the 1970s this legal regime gave way to a different regulatory paradigm.[245] Instead of promoting equal treatment and reliable service, the new framework sought to encourage competition both among providers and within their forms of service, the idea being that maximizing consumer choice would minimize the need for regulatory involvement.[246] The specific way lawmakers applied this new framework varied by industry. The Airline Deregulation Act of 1978, for example, ended the public utility approach to regulating airlines,

---

239. See id. at 1334 (arguing that, in the 1930s, it was "generally accepted that an administrative system based on filed tariffs" was an effective way of regulating public utilities and common carriers).

240. See id. (noting that some traditionally regulated industries were natural monopolies, while "others were highly competitive"); see also Thomas B. Nachbar, The Public Network, 17 CommLaw Conspectus 67, 97 (2008) ("The early history of common carrier regulation is devoid of any mention of monopoly, nor is market power an element of modern common carrier regulation of many industries. For instance, inns have traditionally been subject to the same liability in the presence or absence of competition." (footnote omitted)).

241. Munn v. Illinois, 94 U.S. 113, 130 (1876) (internal quotation marks omitted) (quoting Sir Matthew Hale, De Portibus Maris, *in* 1 A Collection of Tracts Relative to the Law of England 45, 78 (Francis Hargrave ed., 1787)); see also Nachbar, supra note 240, at 106 ("The object of the business, not the number of competitors in the market, renders one's work public."); Tim Wu, Why Have a Telecommunications Law? Anti-Discrimination Norms in Communications, 5 J. on Telecomm. & High Tech. L. 15, 31 (2006) ("[I]t is the role the carrier plays in the economy that necessitates duties of common carriage, not necessarily the potential for abuse of market power.").

242. See Nachbar, supra note 240, at 85 ("Society's willingness to engineer markets in order to provide access to certain articles of commerce depends in some measure on the necessity of those items.").

243. Id. at 102.

244. Id. at 109.

245. See Kearney & Merrill, supra note 232, at 1325 ("This legal regime has been giving way over the last quarter-century to a very different paradigm.").

246. Id. at 1361.

while the Telecommunications Act of 1996 loosened some restrictions and introduced a new set of requirements oriented around the goal of promoting competition.[247] Across industries, tariffed services, integrated service packages, and regulatory control were abandoned in favor of individually negotiated contracts, unbundled services, and an abridged role for administrative agencies.[248]

The transition away from the traditional regulatory paradigm took place against a background assumption that antitrust laws would robustly police formerly regulated dominant firms. Both Alfred Kahn and then-Professor Stephen Breyer, strong advocates of the shift in regulatory paradigm, described the new regime as a distinct form of regulation.[249] And while most tools of the first regulatory paradigm (rate-setting, for example, or mandated universal service) were largely eliminated in favor of the new competition-based paradigm, structural restrictions on business have remained a feature of both. This is because even as the new model was less directly interventionist, it still relied on the antitrust laws to police markets—and structural limits have been a key remedy in antitrust.[250]

The antitrust laws broadly prohibit anticompetitive conduct and anticompetitive mergers. Structural prohibitions can apply in both contexts. When a company is found to be monopolizing or attempting to monopolize a market in violation of Section 2 of the Sherman Act, breakup of the company is an available remedy.[251] Separately, when a court determines that the effect of a particular merger or acquisition "may be substantially to lessen competition, or to tend to create a monopoly" in violation of Section 7 of the Clayton Act, it can enjoin

---

247. See id. at 1325–26, 1335.

248. Id. at 1326.

249. This view was captured by Alfred Kahn, a primary architect of airline deregulation. In an interview he reflected on the thinking at the time: "[The Airline Deregulation Act] provided for eventual total deregulation on route, entry and exit . . . and total freedom of pricing. It did not eliminate antitrust scrutiny. . . . [O]f course we continued to regulate with intensified application of the antitrust laws." Alfred E. Kahn Interview, PBS: The First Measured Century, http://www.pbs.org/fmc/interviews/kahn.htm [https://perma.cc/GN6Q-SX5E] (last visited Oct. 19, 2018); see also Stephen Breyer, Analyzing Regulatory Failure: Mismatches, Less Restrictive Alternatives, and Reform, 92 Harv. L. Rev. 547, 578 (1979) [hereinafter Breyer, Analyzing Regulatory Failure] ("[O]ne should recognize that 'unregulated' markets are subject to the antitrust laws—a form of government intervention designed to maintain a workably competitive marketplace.").

250. As then-Chief Judge Breyer put it, "[e]conomic regulators seek to achieve [the goals of low prices, innovation, and efficient production methods] *directly* by controlling prices through rules and regulations; antitrust seeks to achieve them *indirectly* by promoting and preserving a [competitive] process that tends to bring [these goals] about." Town of Concord v. Bos. Edison Co., 915 F.2d 17, 22 (1st Cir. 1990).

251. See, e.g., Standard Oil Co. of N.J. v. United States, 221 U.S. 1, 78 (1911) ("The court below . . . adjudged that the New Jersey corporation . . . was a combination in violation of the 1st section of the [Sherman Act], and an attempt to monopolize or a monopolization contrary to the 2d section of the act. It commanded the dissolution of the combination . . . ."); United States v. Microsoft Corp., 253 F.3d 34, 99–100 (D.C. Cir. 2001) (en banc) (per curiam) (summarizing the district court's remedy, which mandated a structural separation between Microsoft's operating system and browser).

the merger.[252] Compared to separations implemented through regulations, antitrust separations are less likely to categorically deny market entry, although consent decrees that govern a significant market segment may achieve that effect.[253] In either case, the separation intervenes at the level of business structure rather than conduct.[254]

Unknown at the time of the shift away from regulated industries was how drastically antitrust law, too, would be transformed. Through the 1960s, antitrust courts and enforcers assessed business expansion into adjacent markets through "economic structuralism," an approach that analyzed competition primarily through examining the structure of markets.[255] Although the government was light on bringing antitrust actions in vertical merger cases up until the 1930s, scrutiny of vertical expansion picked up after the Great

252. See Mergers, FTC, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/mergers [https://perma.cc/B4FE-N3Q4] (last visited Mar. 17, 2019) ("Merger law is generally forward-looking: it bars mergers that *may* lead to harmful effects.").

253. For example, in United States v. Paramount Pictures, Inc., 334 U.S. 131 (1948), the Justice Department entered into consent decrees with five major motion picture companies and three minor ones. See id. at 141 n.3. Each decree mandated a separation between film distribution and exhibition, requiring those defendants that then owned theatres to divest either their distribution operations or their movie theatres. Barry J. Brett & Michael D. Friedman, A Fresh Look at the *Paramount* Decrees, Ent. & Sports Law., Fall 1991, at 1, 3 ("[S]ome of the majors were required to 'divorce' themselves from their theatre interests and were prohibited from engaging in the exhibition business except upon . . . permission by the court. Similarly, some of the divorced exhibition companies were prohibited from engaging in production and distribution activities without court approval." (footnote omitted)); see also infra section III.D. Meanwhile, in earlier enforcement eras the FTC would routinely enter consent orders prohibiting subsequent acquisitions in particular lines of business. As of 1975, the FTC had at least fifty-four orders with provisions barring acquisitions. See United States v. ITT Cont'l Baking Co., 420 U.S. 223, 250 n.7 (1975) (Stewart, J., dissenting).

254. Separate from government-mandated separations, sometimes firms break themselves up. For example, in recent years General Electric has spun off its transportation business and its healthcare unit, and—in a breakup partially reflecting the separations principle—is separating its natural gas unit from its unit producing equipment and distributing electricity. Thomas Gryta, GE Slashes Dividend, Discloses Criminal Probe; Shares Sink, Wall St. J. (Oct. 30, 2018), https://www.wsj.com/articles/general-electric-slashes-quarterly-dividend-to-1-cent-1540896132 (on file with the *Columbia Law Review*). Corporate spinoffs became popular in the 1980s, when improvements in available data and analysis helped investors realize that specialist firms attract higher valuations than rivals within diversified groups. This "conglomerate discount" gave rise to a strategy whereby corporate raiders would buy firms with short-term "junk" debt that they would repay by selling business units off individually. Stephen Wilmot, Break Up And Die: Why Spinoff Fever Can't Last Forever, Wall St. J. (Nov. 13, 2017), https://www.wsj.com/articles/break-up-and-die-why-spinoff-fever-cant-last-forever-1510580248 (on file with the *Columbia Law Review*). Indeed, corporate spinoffs can generate significant value; one study found that companies divested from parents between 2001 and 2012 "generated a return 17.1 percent in excess of the benchmark over the 22 months following the split." Id. But the spinoffs fared worse than the benchmark during the financial crisis and the Eurozone debt crisis, suggesting that "[i]nvesting in spin offs is essentially a high-risk, high-return strategy." Id. In 2015, the value of corporate spinoffs totaled over $175 billion. Id.

255. See Lina M. Khan, Amazon's Antitrust Paradox, 126 Yale L.J. 710, 717–22 (2017) [hereinafter Khan, Antitrust Paradox] ("One of the most significant changes in antitrust law and interpretation over the last century has been the move away from economic structuralism.").

Depression, which wiped out thousands of small unintegrated businesses and catalyzed a political movement against integrated chain stores.[256]

Skeptics of vertical integration offered two primary theories of harm: leverage and foreclosure. The concern with leverage was that a dominant firm would use its market power in one line of business to establish an outsized advantage in an adjacent market.[257] The risk posed by foreclosure meanwhile was that a vertically integrated firm would compel its subsidiary to deal exclusively with the parent, depriving unintegrated rivals of access to the firm's good or service.[258] At a minimum, critics worried that vertical integration increased barriers to entry by necessitating potential entrants to compete in both lines of business.

In 1950, Congress amended Section 7 of the Clayton Act to make it expressly applicable to vertical acquisitions.[259] Through the 1970s, the Justice Department successfully challenged vertical deals, resulting in divestitures.[260] Ruling that a merger between a major producer and leading retailer of shoes would undermine competition, the Supreme Court explained that

> [t]he primary vice of a vertical merger or other arrangement tying a customer to a supplier is that, by foreclosing the competitors of either party from a segment of the market otherwise open to them, the arrangement may act as a 'clog on competition,' which deprive(s) rivals of a fair opportunity to compete.[261]

And in holding that the second largest auto manufacturer's acquisition of a leading auto parts dealer would foreclose market access for independent dealers, the Court concluded that "only divestiture would correct the condition

---

256. Herbert Hovenkamp, Robert Bork and Vertical Integration, 79 Antitrust L.J. 983, 985–88 (2014) [hereinafter Hovenkamp, Vertical Integration] (noting that, before the 1930s, "the Supreme Court wholeheartedly approved vertical integration that was not found to be part of a monopolization scheme"); see also id. at 986 ("[V]ertical integration leads to production cost savings and, to a lesser extent, savings in transaction costs. The belief that vertical integration had much to do with economy and little to do with monopoly dominated the thought of both the classical political economists and early neoclassical economics.").

257. See, e.g., Friedrich Kessler & Richard H. Stern, Competition, Contract, and Vertical Integration, 69 Yale L.J. 1, 16 (1959) (explaining that "horizontal power in one market or stage of production creates 'leverage' for the extension of the power to bar entry at another level," such that a vertically integrated dominant firm could "impair competition to a greater extent than could the exercise of horizontal power alone").

258. See id. at 14 ("Vertical integration, whether by contract or ownership, necessarily forecloses access to a segment of the market, since competitors of the integrating firm often can no longer deal with the integrated enterprise.").

259. Clayton Act, ch. 1184, § 7, 64 Stat. 1125, 1125–26 (1950) (codified as amended at 15 U.S.C. § 18 (2012)).

260. See, e.g., Ford Motor Co. v. United States, 405 U.S. 562, 578 (1972) (requiring the dissolution of a vertical acquisition by Ford, a major automobile manufacturer, of assets from an automotive parts manufacturer).

261. Brown Shoe Co. v. United States, 370 U.S. 294, 323–24 (1962) (citation omitted) (quoting Standard Oil Co. of Cal. v. United States, 337 U.S. 293 (1949)).

caused by the unlawful acquisition."[262] Though enforcers' analysis of vertical control—through ownership or contract—was case-specific, it was integration by *dominant* firms that was most commonly held to be anticompetitive, given that exclusionary conduct by dominant companies could, in practice, entirely close off markets to unintegrated rivals.[263] In *United States v. E.I. du Pont de Nemours & Co.*, the Court held that internal transfers within a vertically integrated firm could be anticompetitive if they denied competitors market access.[264] And in the 1968 Merger Guidelines, the Justice Department stated that integration achieved through a large vertical merger "will usually raise entry barriers or disadvantage competitors to an extent not accounted for by, and wholly disproportionate to, such economies as may result from the merger."[265]

This approach to vertical integration underwent a sea change during the 1980s. Though some economists had for decades maintained a benign view of vertical integration, it was work by Robert Bork, Ward Bowman, and Richard Posner, among others, that helped drive an overhaul in policy.[266] Bork's

---

262. Ford Motor Co. v. United States, 405 U.S. 562, 575 (1972); see also id. at 571 ("Every extended vertical arrangement by its very nature, for at least a time, denies to competitors of the supplier the opportunity to compete for part or all of the trade of the customer-party to the vertical arrangement." (quoting *Brown Shoe*, 370 U.S. at 323–24)).

263. Reflecting this view, Professors Carl Kaysen and Donald Turner—two influential antitrust thinkers—criticized vertical integration in concentrated markets, connecting integration to monopolistic outcomes. See Carl Kaysen & Donald F. Turner, Antitrust Policy: An Economic and Legal Analysis 120–21 (1959).

264. See 353 U.S. 586, 605–07 (1957) ("The statutory policy of fostering free competition is obviously furthered when no supplier has an advantage over his competitors from an acquisition of his customer's stock likely to have the effects condemned by [Section 7 of the Clayton Act].").

265. U.S. Dep't of Justice, 1968 Merger Guidelines 9–10 (1968), https://www.justice.gov/sites/default/files/atr/legacy/2007/07/11/11247.pdf [https://perma.cc/B6HW-4Q8L].

266. Earlier in the century, prominent economists including John Maurice Clark and Ronald Coase had stressed that vertical integration can produce significant cost savings. See John Maurice Clark, Studies in the Economics of Overhead Costs 81, 136–41 (1923) (noting that vertical integration yields "important economies to be had, distinct from the other economies of large-scale production"); R.H. Coase, The Problem of Social Cost, 3 J.L. & Econ. 1, 16–19 (1960) (explaining that one of the benefits of vertical integration is that "individual bargains between the various cooperating factors of production are eliminated"). Economists who instead emphasized the harmful effects of vertical integration included Joe Bain, Arthur Burns, Edward Chamberlain, and Henry Simons. See Joe S. Bain, Industrial Organization 514–17 (1959) ("Potentially inherent in almost any structure of vertically integrated firms are some implicitly exclusionary effects, or some virtual disadvantages to actual or potential competitors of the integrated firms."); Arthur R. Burns, The Decline of Competition: A Study of the Evolution of American Industry 431–45 (1936) (discussing the consequences of vertical integration, chief among them that vertical integration "diminishes the effectiveness of the market as a stimulus to the improvement of methods of production"); Edward Chamberlain, The Theory of Monopolistic Competition 122–23 (1933) (arguing that one firm's decision to vertically integrate incentivizes other firms to do the same, resulting in "duplication of distributive machinery" and "still more waste"); Henry C. Simons, A Positive Program for Laissez Faire 20–21 (Harry D. Gideonse ed., Public Policy Pamphlets No. 15, 1934) ("[V]ertical combinations (integration) should be permitted only so far as clearly compatible with the maintenance of real competition. Few of our gigantic corporations can be defended on the ground that their present size is necessary to reasonably full exploitation of production economies . . . ."). For a general overview of economic attitudes toward vertical

scholarship challenged both the leverage and foreclosure theories of harm as logical fallacies,[267] while Bowman argued that the jurisprudence around tying agreements was deeply flawed.[268]

These scholars, associated with the Chicago School, argued that, contrary to prevailing economic theory and antitrust policy, vertical integration was almost always procompetitive. This view was premised primarily on three arguments. First, they maintained, firms could not extract additional profits from extending a dominant position into a distinct market, because—assuming that a firm was already selling a combination of goods at its profit-maximizing price—increasing the price of one would result in a corresponding offset in the other.[269] Second, the Chicago School held that an integrated firm would be able to foreclose rivals only to the degree that the firm had generated cost savings, outdoing less efficient competitors—an outcome that antitrust should encourage.[270] Insofar as a vertically integrated entity did cut off both upstream sellers and downstream customers, those firms now had an opportunity to transact with one another. And third, they argued, vertical mergers would invariably generate significant efficiencies.[271] Because the upstream division would transfer its input to the downstream entity at marginal cost rather than at a sales price, vertical mergers eliminated double marginalization, leading the downstream partner to lower prices for consumers.

With the election of President Reagan, these theories were stamped into policy through both the antitrust agencies and federal judiciary. For the next decade, antitrust officials did not challenge a single vertical merger and relaxed scrutiny of vertical restraints more generally.[272] The transformation in how

---

integration through the Great Depression, see Herbert Hovenkamp, Enterprise and American Law, 1836–1937, at 331–48 (1991).

267. See Robert H. Bork, The Antitrust Paradox: A Policy at War with Itself 231–38 (1978) [hereinafter Bork, Antitrust Paradox] (claiming that the "sole merit" of the foreclosure theory of harm "is that it establishes a new high in preposterousness"); Robert H. Bork, Vertical Integration and the Sherman Act: The Legal History of an Economic Misconception, 22 U. Chi. L. Rev. 157, 195–201 (1954) (arguing against the leverage theory of harm because "it is always horizontal market power, and not integration into other levels" that determines a firm's ability to earn monopoly profits).

268. See Ward S. Bowman, Jr., Tying Arrangements and the Leverage Problem, 67 Yale L.J. 19, 19–20 (1957) ("Present legal methods of treating tying contracts are based upon a false notion of leverage.").

269. See supra section I.E.2; see also, Bork, Antitrust Paradox, supra note 267, at 229; Bowman, supra note 268, at 25.

270. See Bork, Antitrust Paradox, supra note 267, at 236–37.

271. See id. at 219; Joseph J. Spengler, Vertical Integration and Antitrust Policy, 58 J. Pol. Econ. 347, 347–52 (1950) ("Vertical integration, on the contrary, does not, as such, serve to reduce competition and may, if the economy is already ridden by deviations from competition, operate to intensify competition.").

272. See Steven C. Salop, Reinvigorating Vertical Merger Enforcement, 127 Yale L.J. 1962, 1964 (2018) (noting that the last vertical merger case litigated to completion by the FTC occurred in 1979). This shift in policy was also reflected in the 1982 Merger Guidelines. Compare U.S. Dep't of Justice, 1968 Merger Guidelines (1968), https://www.justice.gov/sites/default/files/atr/legacy/2007/07/11/11247.pdf

antitrust authorities approached vertical structures and conduct was part of a broader revolution in antitrust law, which embraced "consumer welfare" as the lodestar of antitrust and adopted price theory as the proper methodology for analyzing competition.[273] As courts incorporated this new learning into their analysis, they shifted from rules to standards, narrowing the range of dominant firm conduct treated as anticompetitive.[274] Although the Chicago School's influence drove these changes at the level of policy, the Harvard School—whose prominent members included Phil Areeda and Stephen Breyer—also played a critical role in setting the intellectual foundation for narrowing the zone of liability for dominant firms.[275]

Since the Chicago School's "resounding victory," scholars have critiqued some of its excesses and moderated its theories, delivering the "Post-Chicago School."[276] Today's approach to antitrust law largely follows in this Post-Chicago tradition, where Chicago's influence has been tempered even as it remains indelible.[277] The following section reviews the current antitrust approach to vertical integration and why it risks neglecting potentially anticompetitive vertical conduct by dominant platforms.

B. *Contemporary Antitrust's Treatment of Vertical Integration*

Most forms of vertical integration today are "viewed as economically beneficial and competitively benign."[278] Antitrust scrutiny of vertical integration has two legal hooks: (1) Section 7 of the Clayton Act, which states that mergers that may "substantially lessen competition" are unlawful,[279] and (2) Section 2 of the Sherman Act, which prohibits monopolization or attempted monopolization.[280] An unlawful vertical merger could be challenged under Section 7, and vertical conduct that constitutes monopolization or attempted

---

[https://perma.cc/XTB6-E92K] (emphasizing market structure), with U.S. Dep't of Justice, 1982 Merger Guidelines (1982), https://www.justice.gov/sites/default/files/atr/legacy/2007/07/11/11248.pdf [https://perma.cc/YV94-HPH7] (emphasizing price).

273. See William E. Kovacic, The Intellectual DNA of Modern U.S. Competition Law for Dominant Firm Conduct: The Chicago/Harvard Double Helix, 2007 Colum. Bus. L. Rev. 1, 8 (describing modern antitrust law as evincing a "wariness of rules that might discourage dominant firms from pursuing price-cutting, product development, or other strategies that generally serve to improve consumer welfare").

274. See, e.g., id. at 64 (noting that recent antitrust jurisprudence has led to "more permissive substantive liability rules" and has created "non-intervention presumptions of liability standards that constrain the prosecution of private antitrust cases").

275. Id. at 14.

276. See Daniel A. Crane, Chicago, Post-Chicago, and Neo-Chicago, 76 U. Chi. L. Rev. 1911, 1911 (2009) ("Of all of Chicago's law and economics conquests, antitrust was the most complete and resounding victory. . . . [N]ever did Chicago trounce its ideological opponents as plainly and lastingly as it did in the field of its early conquests—antitrust.").

277. For a high-level review of post-Chicago theory on vertical integration, see infra Appendix.

278. Hovenkamp, Vertical Integration, supra note 256, at 996.

279. 15 U.S.C. § 18 (2012).

280. Id. § 2.

monopolization could be targeted under Section 2. Given the dearth of cases challenging vertical mergers, the law governing vertical mergers has remained "undeveloped."[281]

Two factors that inform whether a vertical merger or vertical conduct is held to be anticompetitive are the competitiveness of a market and the presence of entry barriers. Economic analysis holds that foreclosure is a viable antitrust strategy in monopolistic and oligopolistic markets protected by entry barriers.[282] Similarly, establishing monopolization generally requires showing both the existence of monopoly power and the existence of entry barriers.[283]

In digital platform markets, two potential entry barriers worth assessing are network effects and unequal access to data. In markets characterized by network effects, the value of the relevant good or service increases with greater use of that good or service.[284] Whereas supply-side economies of scale reflect declining average and marginal costs of production, network effects are a *demand*-side feature. Depending on the type and strength of the network effects, these externalities can serve as barrier to entry—a finding that formed the basis of the *Microsoft* decision.[285] Scholarship analyzing the conditions under which unequal access to data serves as an entry barriers is still developing, but initial work suggests that the self-reinforcing advantages of data may give incumbents a sufficiently significant lead that potential competitors struggle to enter.[286]

---

281. Salop, supra note 272, at 1964–65; see also United States v. AT&T, 310 F. Supp. 3d 161, 192 (D.D.C. 2018) (identifying a lack of clear precedent in the application of antitrust principles to vertical merger cases).

282. See Thomas G. Krattenmaker & Steven C. Salop, Anticompetitive Exclusion: Raising Rivals' Costs to Achieve Power over Price, 96 Yale L.J. 209, 224–38 (1986).

283. United States v. Microsoft Corp., 253 F.3d 34, 51, 82 (D.C. Cir. 2001) (en banc) (per curiam). Strikingly, vertical tying by a firm with market power is still per se illegal. Jefferson Parish Hosp. Dist. No. 2 v. Hyde, 466 U.S. 2, 9–10 (1984).

284. Michael L. Katz & Carl Shapiro, Network Externalities, Competition, and Compatibility, 75 Am. Econ. Rev. 424, 424 (1985); see also Carl Shapiro & Hal R. Varian, Information Rules: A Strategic Guide to the Network Economy 173–74 (1998) (providing an example of positive feedback in network effects by describing how the value of Microsoft and Intel computing systems outpaced the value of Apple computing systems in the late 1990s, given the large share of the market captured by Microsoft and Intel).

285. See United States v. Microsoft Corp., 87 F. Supp. 2d 30, 36 (D.D.C. 2000) ("The plaintiffs proved at trial that Microsoft possesses a dominant, persistent, and increasing share of the relevant market. . . . This barrier ensures that no Intel-compatible PC operating system other than Windows can attract significant consumer demand . . . ."); see also *Microsoft*, 253 F.3d at 83.

286. See, e.g., Stucke & Grunes, supra note 26, at 7 (arguing that, although data-driven industries do not necessarily have high barriers to entry in every instance, "[d]ata-driven markets 'can lead to a "winner takes all" result where concentration is a likely outcome of market success'" (quoting Org. for Econ. Cooperation & Dev., Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report 7 (2014) [hereinafter Data-Driven Innovation], https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf [https://perma.cc/6LW9-3WX6])); Daniel L. Rubinfeld & Michal S. Gal, Access Barriers to Big Data, 59 Ariz. L. Rev. 339, 370 (2017) ("[F]irms enjoying data-based advantages will be motivated to engage in exclusionary conduct and erect artificial barriers to entry in order to maintain or strengthen their advantage . . . . [T]he unique characteristics of big-data markets . . .

Given the turn away from structuralism, contemporary antitrust law generally requires that the allegedly anticompetitive merger or conduct have an anticompetitive *effect*, defined as harm to consumer welfare.[287] This welfare-based framework is understood to include not just static concerns about price and output but also dynamic concerns about innovation.[288]

Notably, discrimination and appropriation by dominant tech platforms seem to generate antitrust harms cognizable even within this welfare-based framework. Insofar as platform conduct reduces investment and entrepreneurial activity by independent parties, any subsequent loss in innovation would—in a dynamic efficiency framework—constitute a harm to competition.[289] These dynamics are an echo of *Microsoft*, insofar as it was Microsoft's conduct against Netscape that prompted the Justice Department to bring its antitrust suit alleging that Microsoft's activity "adversely affect[ed] innovation," by "impairing the incentive[s]" of rivals to "undertake research and development" and "impairing the ability" of "competitors to obtain financing."[290]

Some former state enforcers and lawyers have argued that dominant platforms are engaging in exclusionary conduct to acquire and maintain monopoly power in ways reminiscent of Microsoft—but that enforcers have yet to rectify these marketplace harms, due to unfavorable case law in the United States and inadequate remedies by the European Commission.[291]

---

affect the nature, scale, and scope of such competitive effects."); see also Nathan Newman, Search, Antitrust, and the Economics of the Control of User Data, 31 Yale J. on Reg. 401, 418–19 (2014) [hereinafter Newman, Control of User Data] (discussing the barriers to entry, including an up-front investment in data networks, that Bing faces in competing with Google in the online search market).

287. See supra note 273 and accompanying text.

288. Joshua D. Wright, Antitrust, Multi-Dimensional Competition, and Innovation: Do We Have an Antitrust-Relevant Theory of Competition Now?, *in* Competition Policy and Patent Law Under Uncertainty: Regulating Innovation 228, 230 (Geoffrey A. Manne & Joshua D. Wright eds., 2011) ("The emerging consensus appears to be that . . . antitrust should incorporate dynamic efficiencies into the current framework by accounting for the impact of competition to engage in research and development for new or improved goods, services, or processes.").

289. See Baker, supra note 210, at 576; Michael L. Katz & Howard A. Shelanski, Mergers and Innovation, 74 Antitrust L.J. 1, 3–5 (2007); Wright, supra note 288, at 230. For a high-level overview of existing research on whether platform conduct is suppressing innovation, see Noah Smith, Big Tech Sets Up a 'Kill Zone' for Industry Upstarts, Bloomberg (Nov. 7, 2018), https://www.bloomberg.com/opinion/articles/2018-11-07/
big-tech-sets-up-a-kill-zone-for-industry-upstarts (on file with the *Columbia Law Review*).

290. Complaint at 12–13, *Microsoft*, 87 F. Supp. 2d 30 (No. 98-1232), 1998 WL 35241886.

291. See, e.g., Martin Giles, Gary Reback: Technology's Trustbuster, MIT Tech. Rev. (June 27, 2018), https://www.technologyreview.com/s/611488/gary-reback-technologys-trustbuster/ [https://perma.cc/3CLC-QKF3] ("Why is it that we were able to go after Microsoft in the 1990s, and now we're facing almost identical conduct by Google and we can't manage to do anything about it in the US?" (quoting attorney Gary Reback)); Sally Hubbard, The Case for Why Big Tech Is Violating Antitrust Laws, CNN (Jan. 2, 2019), https://www.cnn.com/2019/01/02/perspectives/big-tech-facebook-google-amazon-
microsoft-antitrust/index.html [https://perma.cc/G7T8-U935] ("The nearly 20-year-old case of *US v. Microsoft* illustrates how today's tech giants are breaking the law. . . . Google, Amazon and Facebook are following the same playbook.").

Platform discrimination and appropriation also risk going unaddressed by contemporary antitrust. This is because of both specific doctrinal changes that have significantly narrowed the range of instances in which single-firm conduct rises to an antitrust offense as well as general blind spots of a consumer welfare approach primarily focused on price and output effects.[292] To appreciate the likely neglect of antitrust to these competition harms, it's worth briefly reviewing the doctrinal obstacles to bringing an antitrust case against a dominant tech platform for discrimination or appropriation.

1. *Denial of Access and the Essential Facilities Doctrine.* — Prior to 2004, a dominant tech platform that blocked independent parties in favor of its own goods or services might have been liable under the "essential facilities" doctrine.[293] Under essential facilities, dominant firms that deny other businesses nondiscriminatory access to their unique facilities may incur antitrust liability.[294]

This doctrine traces to the early years of the federal antitrust law, when the Supreme Court interpreted Section 1 of the Sherman Act to impose obligations of equal and nondiscriminatory access.[295] In subsequent decades, the Court interpreted the Sherman Act to require that the only railroad bridge across the Mississippi river grant open and equal access to all rivals;[296] that the Associated Press grant nondiscriminatory membership to publishers that competed with its existing members;[297] and that the sole power company in a region must transmit power generated by rival firms to customers that sought to buy cheaper power from those rivals.[298]

In 1983, the Seventh Circuit formalized essential facilities into a doctrinal test, requiring plaintiffs to establish four elements: (1) the monopolist controls access to an essential facility; (2) the facility cannot be practically or reasonably duplicated by a competitor; (3) the monopolist denies access to a

---

292. Kevin Caves & Hal Singer, When the Econometrician Shrugged: Identifying and Plugging Gaps in the Consumer Welfare Standard, 26 Geo. Mason L. Rev. (forthcoming 2019) (manuscript at 3–5) (on file with the *Columbia Law Review*) ("The first potential blind spot identified here concerns innovation harms. These harms, which might not manifest until future periods, are not readily quantifiable or relatable to a platform's discrimination; thus, exclusionary conduct that generated such harms may not be cognizable under current the rigorous antitrust injury standard.").

293. Notably, the essential facilities doctrine would be available to independent parties only in instances when the dominant platform was a competitor. Denial of access to parties that could not be characterized as competitors would not be cognizable as an essential facilities claim. See, e.g, Olde Monmouth Stock Transfer Co. v. Depository Trust & Clearing Corp., 485 F. Supp. 2d 387, 395 (S.D.N.Y. 2007) ("[T]he essential facility doctrine is intended to prevent a *competitor* from obtaining an unfair advantage in a market by denying to its actual or potential *competitors* access to a facility essential for use of that market.").

294. See, e.g., id.

295. While the Supreme Court has applied the principles underlying the essential facilities doctrine, it has never mentioned it by name. Brett Frischmann & Spencer Weber Waller, Revitalizing Essential Facilities, 75 Antitrust L.J. 1, 6–7 (2008).

296. United States v. Terminal R.R Ass'n of St. Louis, 224 U.S. 383, 411 (1912).

297. Associated Press v. United States, 326 U.S. 1, 21 (1945).

298. Otter Tail Power Co. v. United States, 410 U.S. 366, 378 (1973).

competitor; and (4) it is feasible for the monopolist to provide access.[299] In this way, essential facilities could be seen as "a means of protecting or injecting competition into a market susceptible to monopolization due to structural factors."[300]

Insofar as independent producers or developers could prove these elements, the dominant platform would have been liable.[301] The essential facilities doctrine, however, has died a "death by a thousand cuts,"[302] having drawn academic criticism since the 1980s.[303] As of 2004, the essential facilities doctrine lives in "near extinction."[304] That year, in *Trinko*, the Court ruled on whether a customer of a local phone monopolist could bring an antitrust class

299. MCI Commnc'ns Corp. v. AT&T Co., 708 F.2d 1081, 1132–33 (7th Cir. 1983).

300. Maxwell Meadows, The Essential Facilities Doctrine in Information Economies: Illustrating Why the Antitrust Duty to Deal Is Still Necessary in the New Economy, 25 Ford. Intell. Prop. Media & Ent. L.J. 795, 809 (2015).

301. The first element has two sub-elements that plaintiffs must prove: (1) a defined market in which the defendant has a monopoly over the facility or resource, and (2) the defined market in which the facility is essential. Meadows, supra note 300, at 805. Plaintiffs' success will vary by market, but—given, for example, that Android captures over 85% of the mobile operating systems market and that Amazon captures over 70% of the online book market, see supra note 4—at least some producers would likely prove successful. See, e.g., *MCI*, 708 F.2d at 1133 (finding that the plaintiff had cleared the threshold requirement of showing that the telephone infrastructure at issue constituted "essential facilities" because the plaintiff "could not duplicate [the defendant's] local facilities"). For ideas on how to conceptualize dominant tech platforms and their control over data as "essential facilities," see Meadows, supra note 300, at 813–20 ("The ability to restrict access to either information or means of distribution in their entirety would demonstrate control adequate for the essential facilities doctrine."); see also Zachary Abrahmson, Comment, Essential Data, 124 Yale L.J. 867, 870–72 (2014) (arguing that "a claim to essential data—data essential to competition—should require the same elements as a claim to an essential facility").

302. Frischmann & Waller, supra note 295, at 9.

303. 3B Phillip E. Areeda & Herbert Hovenkamp, Antitrust Law § 771c, at 205 (4th ed. 2015) ("Lest there be any doubt, we state our belief that the essential facility doctrine is both harmful and unnecessary and should be abandoned."). But see James R. Ratner, Should There Be an Essential Facility Doctrine?, 21 U.C. Davis L. Rev. 327, 367–68 (1988) (discussing how the essential facilities doctrine could be "restructured" in response to criticism and arguing that such a restructuring would "contribute meaningfully to the competitive functioning of the downstream market"); Glenn O. Robinson, On Refusing to Deal with Rivals, 87 Cornell L. Rev. 1177, 1183 (2002) (endorsing essential facilities doctrine in lieu of broader general duty to deal for monopolists).

304. Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko LLP, 540 U.S. 398, 410–11 (2004). Professors Brett Frischmann and Spencer Waller note that a narrow view of the Court's skepticism could preserve a version of the essential facilities doctrine for joint refusals to deal under Section 1 of the Sherman Act. Frischmann & Waller, supra note 295, at 9 n.24. Notably, the essential facilities doctrine was criticized by prominent antitrust scholars for decades before *Trinko*. See, e.g., Herbert Hovenkamp, Federal Antitrust Policy: The Law of Competition and Its Practice § 7.7, at 410 (5th ed. 2016) ("The so-called 'essential facility' doctrine is one of the most troublesome, incoherent, and unmanageable bases for Sherman § 2 liability. The antitrust world would almost certainly be a better place if it were jettisoned, with a little fine tuning of the general doctrine . . . to fill any gaps."); Philip J. Areeda, Essential Facilities: An Epithet in Need of Limiting Principles, 58 Antitrust L.J. 841, 852 (1989) (providing "six principles that should limit application of the essential facilities concept").

action challenging discrimination by a monopolist against a rival.[305] Although the Court's holding did not involve essential facilities, in dicta the Court all but rejected the viability of the doctrine.[306] While courts continue to review essential facilities claims, in the wake of *Trinko* no plaintiff has successfully litigated one to judgment.[307]

2. *Discriminatory Refusal to Deal.* — A dominant tech platform that discriminates against those independent parties that provide competing goods or services could, in theory, be liable for discriminatory refusal to deal in violation of Section 2 of the Sherman Act.[308] The key precedent is *Aspen Skiing*, in which the defendant's refusal to sell lift tickets to a rival resort was held to constitute unlawful monopolization.[309] What distinguishes a legitimate refusal to deal from an illegitimate one is whether the dominant firm's actions *discriminate* between rivals and non-rivals.[310] For example, if Android demoted from the Google Play Store apps that competed with Google-owned apps but did not demote non-rivals, the demoted competitors would likely be able to allege a discriminatory refusal to deal claim against Android.

Here, too, the Supreme Court has thrown into doubt the practical viability of unilateral refusal to deal claims. In *Trinko*, the Court denied the existence of any duty to deal and characterized *Aspen Skiing* as "at or near the outer boundary of § 2 liability."[311] Stopping short of foreclosing refusal to deal claims entirely, the Court distinguished *Trinko* from *Aspen Skiin*g on the grounds that (1) *Aspen* involved a defendant that had stopped participating in an existing venture, and (2) the existence of a regulatory structure that already governed the defendant's duty to deal couldn't be reconciled with a separate *antitrust* duty to deal.[312]

The blow of *Trinko* is softened slightly in the context of the dominant tech platforms, which presently are not governed by a separate regulatory regime. But the Court also codified a heightened requirement, establishing that

---

305. See *Trinko*, 540 U.S. at 410–11 (holding that the monopolist's "alleged insufficient assistance" did not create a cognizable antitrust claim).

306. Frischmann & Waller, supra note 295, at 9.

307. Courts have, however, allowed essential facilities claims to proceed beyond summary judgment. See, e.g., Am. Home Healthcare Servs., Inc. v. Floyd Memorial Hosp. & Health Servs., No. 4:17-cv-00089, 2018 WL 1172995, at *7 (S.D. Ind. Mar. 5, 2018).

308. Whereas the essential facilities doctrine only covered instances of denying access, discriminatory refusal to deal covers instances of discriminatory access. See, e.g., *Trinko*, 540 U.S. at 411 ("[W]here access exists, the doctrine serves no purpose."); Aerotech Int'l, Inc. v. Honeywell Int'l, Inc., 836 F.3d 1171, 1185 (9th Cir. 2016) ("Honeywell's ordering process may very well be 'Kafkaeseque,' . . . and Honeywell may even provide priority access to certain customers, [but] Honeywell does not deny Aerotech access to APUs or their component parts.").

309. Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585, 610 (1985).

310. Einer Elhauge, Defining Better Monopolization Standards, 56 Stan. L. Rev. 253, 308–09 (2003) ("[W]hile the ex ante efficiencies created by property rights do justify virtually all refusals to deal on terms other than the price set by the property owner, they do not justify discriminatory refusals to deal with those buyers who are (or deal with) rivals.").

311. 540 U.S. at 409.

312. See id. at 409–12.

discriminatory refusals to deal will only be actionable if the conduct is likely to create a new monopoly or entrench an existing one.[313] In other words, the dominant platform must have a "dangerous probability of success" in monopolizing the adjacent market. Discrimination by Android against independent apps, for example, would constitute a viable claim only if that discrimination were enabling Google to capture a monopolistic share of the relevant app market.[314] Although some commentators have read this requirement as "squeeze[ing] much of the remaining vitality out of Section 2 claims challenging unilateral refusals to deal,"[315] it is possible that platform conduct in certain adjacent markets could be shown to meet even this heightened standard.[316]

3. *Information Appropriation.* — Antitrust enforcers recognize that appropriation of sensitive competitor information can undermine competition. When reviewing vertical mergers, the antitrust agencies assess whether the deal would enable the merging firm to use rivals' information in anticompetitive ways.[317] Enforcers recognize that positioning a dominant firm to collect and analyze a rival-customer's business information could "reduce the incentives of the rivals even to attempt . . . procompetitive moves," resulting in longer-term harm.[318]

Outside of the merger context, appropriation of sensitive business information by a rival is more difficult to cognize as an antitrust harm. Exclusionary conduct cases are generally governed by the rule of reason.[319]

---

313. Id. at 415 n.4; see also Ellen Meriwether, Putting the "Squeeze" on Refusal to Deal Cases: Lessons from *Trinko* and *linkLine*, Antitrust, Spring 2010, at 65, 67.

314. No firm with a market share of less than 50% is a monopolist. Compare United States v. Aluminum Co. of Am., 148 F.2d 416, 424 (2d Cir. 1945) (opining that "it is doubtful whether sixty or sixty-four percent [market share] would be enough" to constitute a monopoly), and Cliff Food Stores, Inc. v. Kroger, Inc., 417 F.2d 203, 207 n.2 (5th Cir. 1969) (observing that more than a 50% market share is a "prerequisite for a finding of monopoly"), with Broadway Delivery Corp. v. United Parcel Serv. of Am., Inc., 651 F.2d 122, 127–29 (2d Cir. 1981) (holding that a 50% market share is not a prerequisite for being a monopolist).

315. Meriwether, supra note 313, at 70 (internal quotation marks omitted).

316. For example, in addition to being a dominant platform in search and mobile operating systems, Google is dominant in several adjacent markets, capturing 59% of the browser market (through Chrome), 81% of the internet maps market (through Google Maps), and 78% of the internet video market (through YouTube). See supra notes 107–108 and accompanying text. Courts generally require a showing of 50% or more market share to establish a "dangerous probability" of success. See, e.g., Actividentity Corp. v. Intercede Grp. PLC, No. 08–cv–04577 VRW, 2009 WL 8674284, at *4 (N.D. Cal. Sept. 11, 2009) (finding that defendant adequately stated an attempted monopolization claim by alleging that plaintiff had more than 50% of the market).

317. Steven C. Salop & Daniel P. Culley, Potential Competitive Effects of Vertical Mergers: A How-To Guide for Practitioners 22–23 (Dec. 8, 2014) (unpublished manuscript) (on file with the *Columbia Law Review*).

318. Id. at 22. Empirical studies suggest that appropriation by dominant platforms is having this effect. See supra section I.E.

319. See, e.g., United States v. Microsoft Corp., 253 F.3d 34, 58–59 (D.C. Cir. 2001) (en banc) (per curiam) (adopting a burden-shifting balancing test for the exclusionary conduct claims

The standard follows a burden-shifting approach: In the first stage, the plaintiff must show a significant anticompetitive effect.[320] If the plaintiff succeeds, then the defendant must demonstrate a legitimate procompetitive justification.[321] If the defendant succeeds in doing so, then the plaintiff can show that the restraint is not reasonably necessary or that the objectives could be achieved by less restrictive alternatives.[322] An empirical study of rule of reason cases found that courts dispose of 97% of cases at the first stage on the ground that there is no anticompetitive effect; courts balance the pro- and anticompetitive effects in only 2% of cases.[323]

An exclusionary conduct case based on information appropriation is especially unlikely to succeed under the current antitrust framework because establishing anticompetitive effects purely on innovation-based harms is extremely challenging under the consumer welfare standard.[324] In part this is because static harms are easier to measure than innovation harms, a fact that tends to bias antitrust analysis towards a focus on price and output effects.[325] In part this is also because dynamic harms can involve significantly greater indeterminacy, such that conduct that yields short-term price reductions might also lead to long-term losses in innovation.

It is true that the Justice Department prevailed in *United States v. Microsoft* by focusing on innovation-based harms.[326] Since *Microsoft*, however, the antitrust agencies have not brought a single case involving a pure-innovation theory of harm in a monopolization case. In the twenty years since, courts have raised evidentiary standards for plaintiffs, demanding "empirical

---

at issue that the court described as being "similar [to the] balancing approach under the rubric of the 'rule of reason'").

320. Id.

321. Id.

322. Id.

323. Michael A. Carrier, The Rule of Reason: An Empirical Update for the 21st Century, 16 Geo. Mason L. Rev. 827, 828 (2009).

324. See Tim Wu, After Consumer Welfare, Now What? The "Protection of Competition" Standard in Practice, Antitrust Chron., Apr. 2018, at 1, 5 [hereinafter Wu, Consumer Welfare], https://www.competitionpolicyinternational.com/wp-content/uploads/2018/04/CPI-Wu.pdf [https://perma.cc/S5FY-QBDS] ("Despite the often brilliant ability of economists to make consumer welfare arguments, the emphasis on measurable harms to consumers still tends to bias the law toward a focus on static harms and, especially, on prices. . . . [This] inevitably tends to marginalize parts of the antitrust law concerned with dynamic harms . . . .").

325. This is more likely to be true in the context of Section 2 enforcement than merger enforcement. Indeed, the antitrust agencies have focused on innovation harms in merger cases. In *United States v. Bazaarvoice, Inc.*, for example, the Department of Justice challenged Bazaarvoice's consummated acquisition of PowerReviews on the theory that the transaction "significantly reduced incentives to . . . invest in innovation." Complaint at 19, United States v. Bazaarvoice, Inc., No. C13-0133 (N.D. Cal. Jan. 8, 2014), 2013 WL 127168.

326. See *Microsoft*, 253 F.3d at 75–76; United States v. Microsoft, 87 F. Supp. 2d 30, 44 (D.D.C. 2000) ("More broadly, Microsoft's anticompetitive actions trammeled the competitive process through which the computer software industry generally stimulates innovation and conduces to the optimum benefit of consumers.").

proof of antitrust impact or injury for consumers that can be directly tied to the conduct."[327] Given both doctrinal hurdles imposed by courts since *Microsoft* as well as the general challenges of concretizing innovation-based harms, a growing set of scholars is concluding that "antitrust generally, and the antitrust agencies specifically, are currently ill-equipped to effectively pursue a platform owner that commands sufficient market power to stifle innovation."[328]

Indeed, the Supreme Court recently made it even more difficult for plaintiffs to successfully allege even price-based anticompetitive effects in certain cases. In *Ohio v. American Express Co.* last term, the Court introduced a special rule for analyzing the conduct of companies operating in "two-sided transaction platforms," requiring that plaintiffs alleging anticompetitive harm on one side of the market must—as part of establishing a prima facie case—*also* show that the purported harm was not offset by benefits on the other side.[329] A drastic departure from traditional forms of antitrust analysis, this "netting" requirement redefines what constitutes anticompetitive conduct in the context of platforms that facilitate a "simultaneous transaction," effectively creating an insurmountable hurdle for plaintiffs.[330] While several commentators—including the Assistant Attorney General for Antitrust—have said they interpret the holding as applying only to a small number of tech platform markets,[331] it is too early to tell whether antitrust defendants will

327. Caves & Singer, supra note 292, at 13.

328. Id. at 10; see also Newman, Control of User Data, supra note 286, at 411–12 (arguing that "earlier and more systematic regulation in new online markets is necessary"); Frank Pasquale, Privacy, Antitrust, and Power, 20 Geo. Mason. L. Rev. 1009, 1010 (2013) ("Antitrust law has been slow to recognize privacy as a dimension of product quality, and the competition that antitrust promotes can do as much to trample privacy as to protect it."); Wu, Consumer Welfare, supra note 324, at 4–5 (questioning whether the consumer welfare standard that is now prevalent in antitrust is "inherently too restrictive and static" to effectively protect competition in the modern world).

329. See 138 S. Ct. 2274, 2287 (2018) (finding that the plaintiffs had failed to meet their burden of demonstrating anticompetitive effects in the credit card market because they based their theory of harm solely on anticompetitive effects on the merchant side of the market without showing any anticompetitive effects in the cardholders' side of the market). The Court held that this novel approach to market definition is warranted when analyzing "transaction platforms," whose key feature, the Court noted, is that "they cannot make a sale to one side of the platform without simultaneously making a sale to the other." Id. at 2277.

330. See Tim Wu, The *American Express* Opinion, the Rule of Reason, and Tech Platforms, 7 J. Antitrust Enforcement 117, 127 (2019) [hereinafter Wu, *American Express*] ("*American Express* suggests that a judge can keep demanding more proof, in concentric lines, until the government's lawsuit collapses"); Lina Khan, America Has a Major Market Power Problem & SCOTUS Just Made It Worse, Take Care Blog (July 5, 2018), https://takecareblog.com/blog/america-has-a-major-market-power-problem-and-scotus-just-made-it-worse [https://perma.cc/VGS3-HYBZ].

331. See Wu, *American Express*, supra note 330, at 118 ("The Supreme Court's opinion does have one great merit as compared to the Second Circuit's: it is narrow, indeed far narrower than some have suggested."); Ina Fried & David McCabe, DOJ Antitrust Official: Supreme Court Ruling Won't Shield Big Tech, Axios (June 26, 2018), https://www.axios.com/makan-delrahim-in-aspen-1530038874-a289ad1a-012b-4ccb-9cb7-69658ee78c33.html [https://perma.cc/6N7K-N5UR] ("[Justice Department Antitrust Chief Makan Delrahim] said that he doesn't think the Supreme Court's American Express ruling would make it more difficult to take on the biggest online platforms over competition concerns.").

successfully expand its reach to cover exclusionary conduct by non-simultaneous transaction platforms.[332]

4. *The Shift Away from Structural Remedies.* — A final trend in antitrust worth identifying is the shift away from structural remedies in vertical merger cases. The 2004 merger guidelines strongly disfavored behavioral remedies.[333] The 2011 guidelines, by contrast, established a preference for a combination of structural and conduct remedies.[334] In practice, the Obama Administration proved reluctant to issue strong structural remedies in vertical cases; it approved two major vertical deals—both described by critics as raising significant anticompetitive concerns—by issuing primarily conduct remedies.[335]

These conduct remedies—in the Ticketmaster–Live Nation and Comcast–NBC mergers—have proved difficult to oversee and enforce.[336] Concerns that Live Nation has failed to abide by the remedies in any meaningful sense have prompted the Justice Department to open a Section 2 investigation, examining whether Live Nation is indeed using its control over concert facilities to pressure customers to also use its ticketing service and retaliating against those who decline its ticket service but still seek access to the concert facility.[337] Comcast, too, has violated the conduct remedies that enforcers imposed when permitting the merger.[338]

These incidents raise broader questions about the relative efficacy and administrative costs of imposing conduct remedies over structural ones.[339] As Professor Spencer Weber Waller has noted, the retreat from structural remedies

---

332. Already, defendants have cited *American Express* in cases not involving simultaneous-transaction platforms. See, e.g., Reply Memorandum of Points and Authorities in Support of Defendant Google LLC's Motion to Dismiss the Complaint Pursuant to Fed. R. Civ. P. 12(b)(6) at 3 n.2, Dreamstime.com, LLC v. Google LLC, No. 3:18-cv-01910 (N.D. Cal. Jan. 28, 2019), 2018 WL 6587482 ("Like the credit card markets discussed in *American Express*, search and search advertising are two-sided in that users are essential to advertisers while ads are essential to finance the system.").

333. Kwoka & Moss, supra note 27, at 980.

334. Id.

335. See Christine Wilson & Keith Klovers, Competition Policy Int'l, Yes We Can, But Should We? Merger Remedies During the First Obama Administration 2 (2014), https://www.competitionpolicyinternational.com/assets/Uploads/WilsonKloverDec-14.pdf [https://perma.cc/DK3M-2RDQ] ("[T]he Agencies revived a number of previously disfavored remedies during the first Obama Administration, including what the Justice Department now characterizes as a 'panoply' of conduct remedies.").

336. Kwoka & Moss, supra note 27, at 1004–07.

337. Ben Sisario & Graham Bowley, Live Nation Rules Music Ticketing, Some Say with Threats, N.Y. Times (Apr. 1, 2018), https://www.nytimes.com/2018/04/01/arts/music/live-nation-ticketmaster.html (on file with the *Columbia Law Review*).

338. Cecilia Kang, FCC: Comcast to Pay $800,000 for Violating NBCU Venture Conditions, Wash. Post (June 27, 2012), https://www.washingtonpost.com/blogs/post-tech/post/fcc-comcast-to-pay-800000-for-violating-nbcu-venture-conditions/2012/06/27/gJQA8MZU7V_blog.html (on file with the *Columbia Law Review*).

339. See generally Kevin J. O'Connor, The Divestiture Remedy in Sherman Act § 2 Cases, 13 Harv. J. Legis. 687, 730–32 (1976) ("Conduct remedies, whether directed primarily at performance results or indirectly at market structure changes, tend to be ineffective.").

has led the antitrust agencies to adopt highly complex remedies that typically "exceed the resources and strengths" of the Justice Department and FTC.[340] Another way to understand the trend is that the agencies have shifted away from structural remedies in favor of remedies that do more regulatory work[341]—even as the agencies are institutionally structured to serve as enforcers rather than regulators.

Stark information asymmetries between enforcers and platforms suggest that enforcing conduct remedies in digital markets will prove even more challenging.[342] Given that rebalancing away from an exclusive reliance on conduct remedies in favor of structural remedies could mitigate these administrability costs and challenges, the case for structural separations in digital markets is worth assessing.

5. *Adjusting Competition to Regulation?* — These trends can be summarized as follows: In the wake of deregulation of network industries and dominant intermediaries, lawmakers expected antitrust to police dominant intermediaries. But in the decades since, courts and enforcers have drastically contracted the basis for antitrust liability in cases involving dominant firms.[343] The result is a highly enfeebled and impoverished set of tools for confronting dominant intermediaries in network industries.

Meanwhile, even innovation harms seem to go unaddressed under the consumer welfare framework, although innovation is central to dynamic efficiency and long-term welfare.[344] In instances when vertical mergers are scrutinized, moreover, growing reliance on conduct remedies has stretched the antitrust agencies beyond their institutional capacities, enabling exclusionary conduct.[345] Notably, the Court has suggested in recent antitrust cases that remedies for injuries that result from dominant firm conduct may be better pursued through a regulatory paradigm rather than through antitrust law—

340. Waller, supra note 20, at 577 ("Many of these remedies would not be needed if the United States focused on policies of vertical separation or structural remedies in monopolization cases, but this has not been the emphasis of either competition or regulatory policy in the United States for decades.").

341. These include: obligations to provide competitors and customers with critical inputs and access to networks on fair and nondiscriminatory terms, the disclosure of necessary intellectual property, the creation of firewalls to discourage the misappropriation of sensitive business information, and the use of special masters and technical committees to oversee dispute resolution. Id. at 576.

342. One facet of this shortcoming is the disadvantage agencies face in policing how firms share and use data. See, e.g., Peter Maass, How a Lone Grad Student Scooped the Government and What It Means for Your Online Privacy, ProPublica (June 28, 2012), https://www.propublica.org/article/how-a-grad-student-scooped-the-ftc-and-what-it-means-for-your-online-privac [https://perma.cc/XGV8-EDAN].

343. See supra notes 272–274 and accompanying text.

344. See supra notes 324–325 and accompanying text.

345. See supra notes 339–341 and accompanying text.

further suggesting that judicial aversion to antitrust will make addressing platform integration through current law extremely challenging.[346]

In light of these trends, the question of whether structural separations should be recovered as a tool of competition policy is salient because digital platform markets seem to favor monopolistic market structures. Growing empirical research shows that dominant tech platforms enjoy uniquely durable market power.[347] Network effects and the self-reinforcing advantages can lead to winner-take-all dynamics, where markets tip early and potential entrants face significant barriers.[348] Expectations that the tech sector would be sufficiently fast-moving and rapidly innovating so as to justify a relatively hands-off approach to antitrust were too rosy.[349]

The question of how to adjust expectations of competition to the reality of its absence has an analogue. As formerly monopolistic sectors were opened up to competition, a wave of scholarship in the 1990s and 2000s explored how the legal regime governing these markets should adjust accordingly.[350] Specifically, these scholars asked: When should an increasingly competitive market lead us to abandon regulations whose justifications depend on monopoly market structure?

What we lack is an understanding of the inverse question: When do we decide that what was perceived as a competitive market in fact is monopolistic

---

346. See Credit Suisse Sec. (USA) LLC v. Billing, 551 U.S. 264, 283–84 (2007) ("[W]here securities regulators proceed with great care to distinguish the encouraged and permissible from the forbidden [and] where the threat of antitrust lawsuits . . . could seriously alter underwriter conduct in undesirable ways, to allow an antitrust lawsuit would threaten serious harm to the efficient functioning of the securities markets."); Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, 540 U.S. 398, 411–12 (2004) ("One factor of particular importance is the existence of a regulatory structure designed to deter and remedy anticompetitive harm. Where such a structure exists, the additional benefit to competition provided by antitrust enforcement will tend to be small . . . .").

347. See infra Part V.

348. See, e.g., Data-Driven Innovation, supra note 286, at 7.

349. Richard A. Posner, Antitrust in the New Economy, 68 Antitrust L.J. 925, 939 (2001) [hereinafter Posner, New Economy] ("The gale of creative destruction that Schumpeter described, in which . . . temporary monopolies operates to maximize innovation that confers social benefits far in excess of the social costs of the short-lived monopoly prices that the process also gives rise to, may be the reality of the new economy.").

350. See, e.g., Howard A. Shelanski, Adjusting Regulation to Competition: Toward a New Model for U.S. Telecommunications Policy, 24 Yale J. on Reg. 55, 57 (2007) [hereinafter Shelanski, Adjusting Regulation] ("The question to be addressed is whether, in the light of changes in telecommunications markets over the past decade, ex ante, dominant-firm restraints remain an appropriate mode of telecommunications regulation."); Daniel F. Spulber & Christopher S. Yoo, Toward a Unified Theory of Access to Local Telephone Networks, 61 Fed. Comm. L.J. 43, 45 (2008) ("This approach taken by Congress and the FCC suffers from several conceptual shortcomings. It overlooks the fact that the emergence of competition undermines many of the basic rationales for regulation."); Kevin Werbach, No Dialtone: The End of the Public Switched Telephone Network, 66 Fed. Comm. L.J. 203, 205 (2014) (arguing that the Public Switched Telephone Network (PSTN) had been "undermined [by] . . . the rise of the Internet; customers and providers abandoning wireline voice telephony; and the collapse of the regulatory theory for data services," and providing "a framework for moving beyond the PSTN").

or oligopolistic, warranting the application of rules traditionally applied to dominant firms? And which traditional tools should apply?

These questions animate this Article, with a focus on one of these tools: structural separations. As Part III will discuss, structural separations have been a mainstay tool applied to network industries and dominant intermediaries. While much of the focus—and criticism—of the public utility regime has centered on rate regulation, vertical separations have been less closely studied.[351] Separations differ from rate regulation and several other regulatory tools in that separations are ex ante rules whose application does not require continuous government intervention or constant monitoring. Insofar as a primary criticism of the public utility era is that many of the regulations proved too unwieldy for courts and enforcers to implement, structural separations appear far more appealing.[352] Contrasted with other public utility tools, separations reduce regulatory burden and reflect humility about the capacity of public officials to manage business conduct.

III. SEPARATIONS REGIMES

This Part provides an overview of five separations regimes, as applied to railroads, bank holding companies, television networks, and telecommunication carriers. Two of these separations were implemented through statute,[353] two through agency regulations,[354] and one as an antitrust remedy.[355]

To be sure, this list is not exhaustive; lawmakers and enforcers have implemented structural prohibitions in a variety of other contexts.[356] This section seeks to offer a representative sample across a few network industries to identify the range of concerns that arise when companies that play an infrastructure role in distribution networks integrate into lines of business that rely on those networks.

A. *Railroads*

By 1900, a handful of railroads had captured the market for anthracite coal. Six firms owned 90% of the total anthracite resources, resulting in high,

---

351. Rahman, New Utilities, supra note 26, at 1638 (discussing how the perceived failures of the public utility approach have been rooted partly in an "overly narrow focus on regulatory rate setting").

352. See Delrahim, supra note 27 (describing non-structural regulatory interventions as requiring the government to serve as "a roving ombudsman into the affairs of business" and noting that "we often don't have the skills or the tools to do so effectively").

353. See infra sections III.A–.B.

354. See infra sections III.C–.D.

355. See infra section III.E.

356. Separations regimes not examined here include provisions of the Glass–Steagall Act, 12 U.S.C. §§ 24, 378 (2012), the Public Utility Holding Company Act, 15 U.S.C. § 79 (2000) (repealed by the Energy Policy Act of 2005, 42 U.S.C. §§ 16451–16463 (2012)), the consent decree in United States v. Paramount Pictures, Inc., 334 U.S. 131(1948), and section 619 of the Dodd–Frank Act, 12 U.S.C. § 1851, known as the "Volcker Rule."

uniform prices and yielding massive profits for the railroads.[357] Through controlling both the tracks and the coal, railroads came to engage in the same kinds of discriminatory conduct that Congress had outlawed through the Interstate Commerce Act.[358] Independent coal companies found, for example, that the railroads refused to provide them with sufficient cars to transport their coal to market,[359] giving the railroad-owned coal superior access to markets.[360]

Seeking to rectify this runaround, Congress included in the 1906 Hepburn Act a provision separating the function of transportation from the function of ownership over goods.[361] While this specific prohibition was introduced last-minute in the Senate and therefore did not generate extensive debate,[362] the concept was not new; a congressional committee in 1892 had undertaken an investigation of the railroad sector and concluded that "the public interest demanded that the business of a common carrier should be absolutely separated from any other."[363]

Known as the "commodities clause," this provision forbade a railroad from carrying "any article or commodity" that it had "manufactured, mined, or produced," or in which it "may have any interest[,] direct or indirect."[364] Under

---

357. Comment, The Judicial History of the Anthracite Monopoly, 41 Yale L.J. 439, 439 (1932).

358. As the Court described,

> [T]he great purpose of the act to regulate commerce, whilst seeking to prevent unjust and unreasonable rates, was to secure equality of rates as to all and to destroy favoritism, these last being accomplished by requiring the publication of tariffs and by prohibiting secret departures from such tariffs, and forbidding rebates, preferences and all other forms of undue discrimination.

N.Y., New Haven, & Hartford R.R. Co. v. Interstate Commerce Comm'n, 200 U.S. 361, 391 (1906).

359. Note, Present Status of the Commodities Clause of the Hepburn Act, 1 St. Louis L. Rev. 59, 59 (1915) [hereinafter Note on Commodities Clause].

360. See, e.g., *Hartford R.R.*, 200 U.S. at 382.

361. See Hepburn Act, Pub. L. No. 59-337, sec. 1, § 1, 34 Stat. 584, 585 (1906).

362. See 40 Cong. Rec. 6455–61, 6493–500, 6551–70, 7011–17 (1906). Discussions from May 7th to May 9th were conducted under the fifteen-minute rule with the Senate in the Committee of the Whole. This was by no means the first time that the separation of transportation and industry had been proposed. This separation had been advocated by an 1834 Pennsylvania legislative report. See Francis Walker, The Development of the Anthracite Combination, 111 Annals Am. Acad. Pol. & Soc. Sci. 234, 236 (1924). The House of Representatives made the same recommendation in 1893. See H.R. Rep. No. 52-2278, at viii (1893).

363. Eliot Jones, The Commodity Clause Legislation and the Anthracite Railroads, 27 Q.J. Econ. 579, 587 (1913).

364. Sec. 1, § 1, 34 Stat. at 585. The full text of the commodities clause reads:

> From and after May first, nineteen hundred and eight, it shall be unlawful for any railroad company to transport from any State, Territory, or the District of Columbia to any other State, Territory, or the District of Columbia, or to any foreign country, any article or commodity, other than timber and the manufactured products thereof, manufactured, mined, or produced by it, or under its authority, or which it may own in whole, or in part, or in which it may have any interest direct or indirect except such articles or commodities as

the original version of the bill, this rule would have applied to all "common carriers," including pipelines for oil, natural gas, and other commodities.[365] But business interests in the oil and gas sector managed to narrow the provision so that the final language emerging from conference covered not common carriers in general but only railroads.[366] Several senators also successfully pushed to exclude timber and lumber from the general prohibition, arguing that a whole group of railroads that had invested in tracks for the sole purpose of transporting lumber would otherwise go bankrupt.[367] More extensive debate and discussion might have yielded a more sweeping ban,[368] had Congress not been "anxious to secure the speedy passage of the bill."[369] The Hepburn Act passed the Senate by 71-3, with fifteen senators not voting.[370]

The backlash from the railroads against the law was almost immediate. States in the anthracite region—including New Jersey, New York, and Pennsylvania—had been encouraging railroads to purchase coal lands in order to develop those states' natural resources.[371] In some cases the states had embedded the right to own coal mines in corporate charters.[372] Following state guidance and incentives, the railroads had invested heavily to purchase coal mines—only to see the Hepburn Act penalize them for it.[373]

Shortly after the bill was enacted, the Attorney General filed suits against six railroad companies that had not divested their coal interests.[374] One firm responded with a constitutional challenge, alleging that the act fell outside congressional authority to regulate interstate commerce and that the

---

> may be necessary and intended for its use in the conduct of its business as a common carrier.

Id.

365. Jones, supra note 363, at 582–83.

366. Id. at 583; see also sec. 1, § 1, 34 Stat. at 585.

367. See Jones, supra note 363, at 582–83.

368. At least one critic argued for extending "'the principle of dissociation'" to "'any two industries that are complementary in their nature'" and maintained that the failure of the United States to "divorce transportation altogether from other enterprises" led to continued monopolization by railroads of other industries. Thurlow M. Gordon, Book Review, 29 Harv. L. Rev. 797, 797–98 (1916) (quoting Thomas Latimer Kibler, The Commodities Clause 147, 162 (1916)).

369. Jones, supra note 363, at 586.

370. Id. at 583.

371. See Note on Commodities Clause, supra note 359. Pennsylvania had even passed a bill entitled, "An act to authorize railroad and canal companies to aid in the development of coal, iron, lumber, and other material interests of the Commonwealth." United States v. Del. & Hudson Co., 213 U.S. 366, 396 n.1 (1909).

372. See Edwin C. Goddard, Comment, The Commodity Clause of the Hepburn Act, 14 Mich. L. Rev. 49, 51 (1915) (noting that railroads "owned coal properties of great value" and that some had been "organized largely to market this coal," operating under charters granted by Pennsylvania).

373. Not all states had been so permissive. Even before the Hepburn Act, a West Virginia statute had made it unlawful for any railroad to engage in the business of buying and selling coal. Id. at 50.

374. Note on Commodities Clause, supra note 359, at 60.

commodities clause would constitute an impermissible "taking" under the Fifth Amendment.[375] The Court rejected this view and clarified that, contrary to the government's position, a carrier may transport goods that it had produced, *so long as* the carrier had clearly divested its ownership of those goods prior to commencing transport.[376] The Court also construed the statute to permit railroads to carry goods produced by a bona fide distinct company in which the railroad was a stockholder.[377]

Three subsequent cases at the Supreme Court would further test the boundaries of the commodities clause. In 1911, the Court held that a railroad using direct stock ownership in a coal company to wield "complete power over the affairs of the coal company, just as if the coal company were a mere department of the railroad," violated the Hepburn Act.[378] Critically, the problem was not stock ownership per se but "the 'commingling of the affairs . . . ,' so as to make both corporations virtually one."[379] Four years later the Court confronted a coal operation that had been spun off as a separate organization yet remained beholden to its former parent railroad.[380] The vice president of the railroad company also served as the president of the coal company, the two firms shared directors and an office building, and the railroad corporation dictated contractual terms to the coal company, effectively prohibiting it from doing business with other entities.[381] The Court held that no single factor was decisive, but ruled that—taken together—the facts proved that "the relation between the parties was so friendly that they were not trading at arm's length."[382] The key question was whether one company had been "converted into a mere agent or instrumentality of the other."[383] Lastly, the Court reviewed a case in which a single holding company owned both a railroad and a coal company, and the railroad company, in turn, was a majority shareholder in the mining company.[384] Upon examining the circumstances, the Court found that the owners had sought the "abdication of all independent corporate action," surrendering to the holding company the "entire conduct of their affairs."[385] Explaining that courts would "look through the forms to the realities of the relation between the companies,"[386] the Court required that the businesses

375. *Del. & Hudson Co.*, 213 U.S. at 386.

376. Id. at 413–15.

377. Id.

378. United States v. Lehigh Valley R.R. Co., 220 U.S. 257, 273 (1911).

379. John G. Love, Note, Interpretation of the Commodities Clause of the Act of Congress Regulating Railroads, 69 U. Pa. L. Rev. 66, 67–68 (1920) (quoting *Lehigh Valley R.R.*, 220 U.S. at 274).

380. See United States v. Del., Lackawanna & W. R.R. Co., 238 U.S. 516, 518–19 (1915).

381. See id.

382. Id. at 529–30.

383. Id. at 529.

384. United States v. Reading Co., 253 U.S. 26, 45–47 (1920).

385. Id. at 61–62.

386. Id. at 63.

separate to establish "entire independence."[387] In doing so, the Court explained that it was "using the antitrust laws to close a gap" in the Hepburn Act," which had banned railroads from owning commodities but not from entering contractual agreements.[388] The Court recognized that railroads could achieve through exclusive contracting what the law forbade them from achieving through integration.[389]

By the 1920s, any unity of control—through stock ownership or by means of a holding company—was recognized as a violation of the Hepburn Act. Rejecting the view that the statute outright prohibited railroads from having *any* ownership interest in the firms whose goods they transported, the Court adopted an approach that assessed the degree of control between the two firms. Any association of management between railway companies and commodity companies was prohibited.[390]

B. *Banking*

A core principle at the heart of banking regulation in the United States is the separation of banking and commerce. This policy of separation traces back to the charter for the Bank of England[391]—an example that the United States looked to when forming its own banks, and a principle that many state banking regimes also adopted.[392] Between 1870 and 1910, the Supreme Court four times upheld rules enjoining banks from owning commercial businesses.[393]

In 1956, the United States codified this separation principle in the Bank Holding Company Act (BHCA).[394] The Act applied to all firms controlling

---

387. Id. at 64.

388. Hovenkamp, Vertical Integration, supra note 256, at 986.

389. Id.; see also *Reading*, 253 U.S. at 60–62.

390. Some questioned whether the Hepburn Act was ultimately successful given that railroads continued to dominate the coal sector. But this was partly attributed to schemes by J.P. Morgan and other large banks to control multiple interests. See Jules I. Bogen, The Anthracite Railroads: A Study in American Railroad Enterprise 240 (1927).

391. See Bernard Shull, The Separation of Banking and Commerce: Origin, Development, and Implications for Antitrust, 28 Antitrust Bull. 255, 259 (1983) ("Separation was initiated, for all practical purposes, with the establishment of the Bank of England in 1694.").

392. See Arthur E. Wilmarth, Jr., Wal-Mart and the Separation of Banking and Commerce, 39 Conn. L. Rev. 1541, 1554–55 (2007). The New York Free Banking Act of 1838, for example, served as a model when Congress amended the National Bank Act in 1864 to limit the scope of power available to banks and specifically to prohibit national banks from acquiring ownership interests in commercial enterprises. Id. at 1558.

393. See Merchs. Nat'l Bank of Cincinnati v. Wehrmann, 202 U.S. 295, 301 (1906) (affirming that national banks do not have the power to take stock in corporations); First Nat'l Bank of Ottawa v. Converse, 200 U.S. 425, 439 (1906) (same); Cal. Bank v. Kennedy, 167 U.S. 362, 366–67 (1897) (same); First Nat'l Bank of Charlotte v. Nat'l Exch. Bank of Balt., 92 U.S. 122, 128 (1875) (same).

394. See S. Rep. No. 91-1084, at 2 (1970) (stating that the 1956 Act was adopted to prevent "a departure from the established policy of separating banking from other commercial enterprises").

multibank holding companies (i.e., two or more banks).[395] Specifically, § 4(a) prohibited banks from acquiring nonbanking companies and required banks covered by the Act to divest any nonbanking subsidiaries within two years of becoming subject to the law.[396] The Act granted banks some latitude: They could own nonbanking subsidiaries whose activities were deemed by the Federal Reserve to be "so closely related to the business of banking or of managing or controlling banks as to be a proper incident thereto."[397] But in practice, the Federal Reserve granted this exception extremely rarely.[398]

Because the BHCA had applied only to *multi*-bank firms, it had created a loophole. By 1970, the six largest banks in the United States had formed one-bank holding companies in order to engage in commercial activities.[399] Responding to this runaround, Congress amended the BHCA to extend its prohibitions to one-bank holding companies.[400] Lawmakers described the revision as a way to "continue our long-standing policy of separating banking from commerce."[401]

Lawmakers and policymakers have appeared willing to also apply the separation to commercial entities. Starting in 2005, Walmart, Home Depot, Target, and several other commercial firms made moves to acquire FDIC-insured industrial loan companies (ILCs), a type of financial entity.[402] Had the FDIC approved the acquisitions, Walmart's financial arm, for example, would have become the primary processor of payments for Walmart.[403] Critics of the deals worried that Walmart would be able to pressure Walmart Bank to ignore credit problems[404] and that Target and Home Depot would make loans to finance exclusive purchases of their own goods.[405] In the face of opposition from business groups, labor unions, community activists, public interest groups, and

---

395. See Bank Holding Company Act of 1956, Pub. L. No. 84-511, § 2(a), 70 Stat. 133, 133 (codified as amended at 12 U.S.C. § 1841(a) (2012)).

396. Id. § 4(a), 70 Stat. at 135 (codified as amended at 12 U.S.C. § 1843(a)).

397. Id. § 4(c)(6), 70 Stat. at 137 (codified as amended at 12 U.S.C. § 1843(c)(8)).

398. See Carl Felsenfeld, The Bank Holding Company Act: Has It Lived Its Life?, 38 Vill. L. Rev. 1, 83–84 (1993) ("The burden of meeting these conditions . . . has weighed heavily upon the banking community.").

399. See Note, Regulating the One-Bank Holding Companies—Precluding Zaibatsu?, 46 St. John's L. Rev. 320, 322 (2012) (describing the trend in the late 1960s for the nation's largest banks to form one-bank holding companies).

400. See 12 U.S.C. § 1841(a)(1) ("'[B]ank holding company' means any company which has control over *any* bank or over *any* company that is or becomes a bank holding company by virtue of this chapter." (emphasis added)).

401. S. Rep. No. 91-1084, at 3 (1970).

402. See Joe Adler, Flashback: When Walmart Wanted a Bank, Am. Banker (Aug. 23, 2017), https://www.americanbanker.com/opinion/when-walmart-wanted-a-bank [https://perma.cc/AD26-9NNA].

403. See Wilmarth, supra note 392, at 1545 (explaining how the proposed Walmart bank would have limited functions, primarily processing customers' payments and converting checks electronically).

404. Id. at 1545–46.

405. Id. at 1595–96.

members of Congress, Walmart withdrew its application.[406] Applications by the other firms were stalled by FDIC's moratorium.[407]

While the Federal Reserve moved to erode the legal wall between banking and commerce in the late 1990s and early 2000s, renewed publicity around 2013 thrust the issue back into the center of policy debate,[408] prompting congressional hearings and a Senate investigation.[409] Scholarship and reporting newly identified the original hazards of permitting our biggest banks to serve as merchants of essential raw materials.[410] In 2016, the Federal Reserve proposed a rule to rein in banks' nonbanking activities and largely return to the earlier regime.[411] Although many of the biggest banks significantly divested their

406. Eric Dash, Wal-Mart Abandons Bank Plans, N.Y. Times (Mar. 17, 2007), https://www.nytimes.com/2007/03/17/business/17bank.html (on file with the *Columbia Law Review*).

407. See Wilmarth, supra note 392, at 1552–53 (detailing the FDIC's decision in January 2007 to extend its moratorium on commercial firms acquiring ILCs).

408. See, e.g., Editorial, Goldman Sachs's Aluminum Pile, N.Y. Times (July 26, 2013), https://www.nytimes.com/2013/07/27/opinion/goldman-sachss-aluminum-pile.html (on file with the *Columbia Law Review*) (expressing concern that "American lawmakers and regulators have removed many of the barriers that historically separated banking and commerce").

409. See Christian Berthelsen & Ryan Tracy, Senate Report: Banks Had Unfair Commodity-Market Advantages, Wall St. J. (Nov. 19, 2014), https://www.wsj.com/articles/senate-report-says-banks-gained-unfair-advantages-in-commodity-markets-1416434539 (on file with the *Columbia Law Review*) ("A U.S. Senate report on commodity-market activities at big Wall Street banks accuses the firms of being so powerful they were able to influence prices, gain trading advantages and put the broader financial system at risk by entering volatile businesses such as uranium trading and coal production."); Examining Financial Holding Companies: Should Banks Control Power Plants, Warehouses, and Oil Refineries?, U.S. Senate Comm. on Banking, Hous., & Urban Affairs (July 23, 2013), https://www.banking.senate.gov/hearings/examining-financial-holding-companies-should-banks-control-power-plants-warehouses-and-oil-refineriesd [https://perma.cc/JWP8-VS67].

410. See Saul T. Omarova, The Merchants of Wall Street: Banking, Commerce, and Commodities, 98 Minn. L. Rev. 265, 297 (2013) (discussing the risks associated with banks' foray into physical commodities markets and noting a "near-absence of reliable, detailed data on the precise nature and full scope of U.S. banking organizations' physical commodity operations"); David Kocieniewski, A Shuffle of Aluminum, but to Banks, Pure Gold, N.Y. Times (July 20, 2013), https://www.nytimes.com/2013/07/21/business/a-shuffle-of-aluminum-but-to-banks-pure-gold.html (on file with the *Columbia Law Review*) ("Wall Street is flexing its financial muscle and capitalizing on loosened federal regulations to sway a variety of commodities markets . . . ."). But at least one scholar has argued for loosening the separation and allowing commercial firms to own banks, in order to "reduce systemic risk" and create a "more diverse and secure banking structure." See Mehrsa Baradaran, Reconsidering the Separation of Banking and Commerce, 80 Geo. Wash. L. Rev. 385, 402 (2012).

411. See Regulations Q and Y; Risk-Based Capital and Other Regulatory Requirements for Activities of Financial Holding Companies Related to Physical Commodities and Risk-Based Capital Requirements for Merchant Banking Investments, 81 Fed. Reg. 67,220, 67,225 (Sept. 30, 2016) (codified at 12 C.F.R. pts. 217, 225); see also The Federal Reserve's Commodities Proposal: Safety and Soundness Regulation, or an Indirect Prohibition?, Gibson Dunn (Sept. 29, 2016), https://www.gibsondunn.com/the-federal-reserves-commodities-proposal-safety-and-soundness-regulation-or-an-indirect-prohibition/ [https://perma.cc/P99B-H9AL] (providing commentary on the Federal Reserve's proposed rule).

commodities holdings in the wake of public attention,[412] the Federal Reserve rule has yet to be finalized.

C. *Television Networks*

As the television industry grew in the 1950s, the sector consolidated around three networks: ABC, CBS, and NBC. These networks owned and operated the majority of television stations and affiliated stations, controlling the distribution of television programs for a majority of the country.[413] They also produced their own programs. Through an investigation into the networks' programming practices, the Federal Communications Commission (FCC) determined that the networks had acquired significant power over the financing, development, and syndication of television programming.[414] The top three networks controlled all aspects of programming, from creating programs to deciding which programs got aired and syndicated.

The FCC reached two main conclusions. First, by virtue of being the only program providers that could reach almost all Americans, the networks enjoyed monopsony power, which they could wield to acquire programming at terms highly unfavorable to producers.[415] Second, the networks also possessed monopoly power, which they could use to withhold programs from independent stations and to grant favorable syndication rights to their network affiliates.[416] The networks were powerful vertically integrated entities that used their heft against both independent programmers and independent stations. The problem, as the FCC saw it, was that the networks' power would have "the effect of limiting the number and variety of programs available to the public, thereby limiting program diversity, contrary to the FCC's much sought after goal."[417]

The FCC followed its investigation with an order that structurally disallowed networks from entering the production and syndication markets.[418] Specifically, the rule prohibited networks from both syndicating any of their own programs and obtaining financial interests in programs created by

---

412. See Dan Fitzpatrick & Christian Berthelsen, J.P. Morgan to Sell Commodities Business, Wall St. J. (July 26, 2013), https://www.wsj.com/articles/SB10001424127887323 61070457863017091292 1006 (on file with the *Columbia Law Review*) ("J.P. Morgan joins rivals Goldman Sachs Group Inc. and Morgan Stanley, which also are seeking buyers for [their physical commodities operations]").

413. Christopher J. Pepe, Comment, The Rise and Fall of the FCC's Financial Interest and Syndicate Rules, 1 Vill. Sports & Ent. L.F. 67, 71–72 (1994).

414. Id.

415. Tamber Christian, The Financial Interest and Syndication Rules—Take Two, 3 CommLaw Conspectus 107, 107 (1995).

416. Id.

417. Id. at 108.

418. See Competition & Responsibility in Network Television Broad., 23 F.C.C.2d 382, 398, para. 30 (1970) (report and order).

independent producers that the networks aired.[419] By separating production and distribution, these structural rules sought to curb the conflicts of interest created through integration.

Almost from inception, these "fin-syn" rules faced pushback from industry, which lobbied the FCC to revise its order. In a follow-up inquiry in 1978, the FCC observed that the rise of satellite technology had opened up the market to new networks, potentially rendering the 1970 prohibitions obsolete.[420] News that the FCC was considering modifying its order prompted a major advocacy effort by the major motion picture studios, which benefited from limits placed on the networks' activities.[421] Hollywood's interests found a friend in the Reagan Administration, and the FCC kept the 1970 rules in place for another decade. In the early 1990s, the FCC once again moved to review the fin-syn regime, this time issuing revised rules that loosened restrictions on networks' ability to own and syndicate programming.[422] After the Seventh Circuit struck down the rules for being arbitrary and capricious,[423] the FCC responded by issuing rules that imposed on the networks minimal structural restrictions that would phase out in two years.[424] In 1995, the FCC released an order observing that the advent of cable, VCR, and direct broadcasting had opened up the market and loosened the networks' gatekeeper power, resolving concerns about their ability to undermine diversity.[425] Its 1995 order effectuated the end of the fin-syn rules.

D. *Telecommunications: Maximum Separation*

By the 1960s, advances in computing had given rise to a new industry: data processing. Data-processing services relied on communications lines run by telephone monopolies.[426] As telecom carriers began to enter data processing, officials worried that the carriers would use their control over the pipes to squash

419. Id.; see also Marc L. Herskovitz, Note, The Repeal of the Financial Interest and Syndication Rules: The Demise of Program Diversity and Television Network Competition?, 15 Cardozo Arts & Ent. L.J. 177, 183 n.43 (1997).

420. Herskovitz, supra note 419, at 184.

421. See id. at 192.

422. 47 C.F.R. §§ 73.658(k), 73.659–-73.662, 73.3526(a)(11) (1991).

423. Schurz Commc'ns, Inc. v. FCC, 982 F.2d 1043, 1055 (7th Cir. 1992).

424. Evaluation of the Syndication and Financial Interest Rules, 8 FCC Rcd. 3282, 3282–84, para. 1 (1993) (second report and order).

425. Network Financial Interest and Syndication Rules, 60 Fed. Reg. 48,907, 48,907–08 (Sept. 21, 1995) (codified at 47 C.F.R. pt. 73).

426. Robert Cannon, The Legacy of the Federal Communication Commission's Computer Inquiries, 55 Fed. Comm. L.J. 167, 168–69 (2003) ("[T]hese computer network services were dependent upon the underlying communications network. Thus, the unregulated computer services were simultaneously substitute services for the traditional regulated communications network and also dependent upon them.").

nascent rivals.[427] To examine the issue, the FCC launched a series of proceedings called the "Computer Inquiries."

In the first proceeding (*Computer I*),[428] the FCC focused on whether to regulate the data-processing industry and whether to limit common carriers from expanding into the new market.[429] The FCC concluded that the data-processing market was highly competitive, innovative, and characterized by low entry barriers, therefore demonstrating no need for regulation.[430] The reliance of data processing on incumbent carriers, however, posed a risk.

Concerned that carriers would stifle data processing, the FCC adopted a policy of "maximum separation," under which regulated communication carriers could enter the unregulated data-processing market only through a fully separate subsidiary.[431] Carriers *could* do business with their data-processing affiliates but were prohibited from discriminating among affiliates "in the offering of facilities or services, in the timing of the installation of facilities, in the quality of service offered or in the charges for like services."[432] The rule also prohibited carriers from promoting the data-processing services offered by their subsidiaries or from using any excess network capacity to provide data-processing services.[433] Affiliated subsidiaries, meanwhile, were not allowed to own transmission services and instead had to acquire them on a service

427. Id. at 170 ("These enhancements, however, also threatened to be a substitute for regulated services, and regulated services threatened to be a bottleneck in the way of the growth of these services.").

428. Interdependence of Comput. & Commc'ns Servs. & Facilities (*Computer I*), 28 F.C.C.2d 267 (1971) (final decision and order).

429. Note, The FCC Computer Inquiry: Interfaces of Competitive and Regulated Markets, 71 Mich. L. Rev. 172, 172 (1972) [hereinafter Note on FCC Computer Inquiry].

430. See id. at 172–73 (describing the FCC's decision not to regulate the data-processing industry).

431. In the order outlining the new policy, Commissioner Bartley wrote separately that he believed the proposal should require a complete separation of the companies and not permit independent affiliation: "I would go further and require . . . a complete separation of companies making public offerings of regulated common carrier communication services and non-regulated data processing services." *Computer I*, 28 F.C.C.2d at 290 (final decision and order) (Bartley, Comm'r, concurring). This policy did not apply to Bell System, which the FCC felt was already prohibited by the 1956 Consent Decree from entering any unregulated activity (including data processing). Id. at 281–82, paras. 39–40 (majority opinion). Specifically, the FCC mandated that a carrier looking to offer data-processing services: "[(1)] establish a separate data processing corporation, [(2)] have separate accounting books, [(3)] have separate officers, [(4)] have separate personnel, and [(5)] have separate equipment and facilities." Cannon, supra note 426, at 178.

432. *Computer I*, 28 F.C.C.2d at 274, para. 22 (final decision and order). Notably, the FCC's "maximum separation" regime partially mirrors the consent decree imposed on IBM by the Justice Department in 1956. See United States v. Int'l Bus. Mach., 1956 Trade Cas. (CCH) ¶ 68,245 (S.D.N.Y. 1956). That decree required IBM to sell data-processing services through a subsidiary that could be treated no differently than an independent data processor. See Peter Passell, I.B.M. and the Limits of a Consent Decree, N.Y. Times (June 9, 1994), https://www.nytimes.com/1994/06/09/business/ibm-and-the-limits-of-a-consent-decree.html (on file with the *Columbia Law Review*). As part of its compliance, IBM created a separate division. Id.

433. *Computer I*, 28 F.C.C.2d at 274–75, paras. 21, 24 (final decision and order).

basis.[434] These structural safeguards sought to create "an open communications platform available to all users on a nondiscriminatory basis."[435] Recognizing that discrimination by the largest firms posed the most serious risk to competition, the "maximum separation" regime applied only to carriers with annual operating revenues exceeding one million dollars.[436]

Through basing the separation on the distinction between data processors and carriers, the FCC created a loophole for hybrid services that provided both the processing and transportation of data.[437] Initially the FCC held that, so long as the data processing was "incidental" to the communications service, the entire activity would be treated as communications.[438] But the hybrid category continued to pose problems for the FCC, prompting the agency to revisit its rules.[439]

In the late 1970s the FCC undertook a second round of inquiries (*Computer II*).[440] This time the FCC created a new distinction between "basic service" (which referred to pure transmission) and "enhanced service" (which rode the pipes of the "basic service" and included email, voice mail, the internet, newsgroups, interactive voice response, and protocol processing).[441] The FCC maintained its basic conclusion: that "enhanced services" should remain unregulated and that permitting "basic services" into the new market for enhanced services would risk stifling competition in this adjacent market.[442] In response to claims that structural separations on *all* carriers were "inefficient," the FCC raised the size threshold requirement, leaving only AT&T and GTE subject to the ban.[443] All other carriers had to comply with unbundling rules—

434. See id. at 271, para. 16; *Computer I*, 28 F.C.C.2d 291, 303, para. 42 (1970) (tentative decision).

435. Cannon, supra note 426, at 180.

436. Id. at 179. Notably, the FCC did not adopt a separations regime across the board; it cared about understanding the industry dynamics and ensuring that the Commission tailored remedies that actually addressed the problem. In the case of "hybrid services"—service offerings that integrated data processing and message transmission, *Computer I*, 28 F.C.C.2d at 287 (final decision and order)—the FCC decided to take a more case-by-case approach, explaining that "we have insufficient experience with such offerings to enable us to adopt rules of general applicability sufficiently definitive to accommodate the variety of further service offerings." Id. at 276, para. 27.

437. *Computer I*, 28 F.C.C.2d at 287 (final decision and order).

438. *Computer I*, 28 F.C.C.2d at 305, para. 42 (tentative decision).

439. See Susan P. Crawford, Transporting Communications, 89 B.U. L. Rev. 871, 892–94 (2009) (describing how, in *Computer II*, the FCC used a broader definition of "enhanced services" to avoid the definitional problems that plagued the "hybrid" services regime).

440. Amendment of Section 64.702 of the Comm'n's Rules and Regulations (*Computer II*), 77 F.C.C.2d 384 (1980) (final decision).

441. Cannon, supra note 426, at 183–88 (quoting *Computer II*, 77 F.C.C.2d at 420, para. 96).

442. *Computer II*, 77 F.C.C.2d at 387, paras. 5–7; see also id. at 463, para. 208 (discussing costs and benefits to separating regulated basic services from unregulated enhanced services).

443. See id. at 482, para. 251 ("[W]e have determined that AT&T's and GTE's dominant position in the terminal equipment market requires some special treatment . . . . [A] separation requirement might be unduly costly, but we do not contemplate applying the requirement to the small carriers.").

separating basic from enhanced services—but were otherwise allowed to maintain joint operations.[444]

The Commission undertook a third round of investigations (*Computer III*) in 1985.[445] The inquiry was prompted by the FCC's determination that the second round of inquiries had imposed "significant costs on the public in decreased efficiency and innovation."[446] In 1986, the Commission issued its new plan: require carriers to ensure that their network remain open to all users of the basic services, by permitting users to interconnect to certain network functions and interfaces on an "unbundled and equal access basis."[447] In other words, the new rule allowed common carriers to enter computing, so long as they offered unbundled basic service, adopted interconnection, and adhered to special accounting practices to prevent subsidization across lines of business.[448] Over the course of the Computer Inquiries, the FCC switched from structural separation to an unbundling and equal-access regime.[449]

Twice the Ninth Circuit struck down the FCC's move, finding that the Commission "had not adequately explained its apparent 'retreat' from requiring 'fundamental unbundling.'"[450] Absent compelling justification, the court worried that this halfway unbundling regime would fail to prevent the Bell Operating Companies (BOCs) from engaging in discrimination.[451] Meanwhile, the FCC passed an Interim Order that allowed BOCs to provide some computing services without a separate subsidiary.[452] The regime remained in place until the Telecommunications Act of 1996, which undid some of the restrictions on dominant networks in favor of competition.[453]

---

444. See id. at 388–89, para. 12.

445. Amendment of Section 64.702 of the Comm'n's Rules and Regulations (*Computer III*), 104 F.C.C.2d 958, 962, para. 1 (1986) (report and order).

446. Id. at 964, para. 3.

447. Id. at 1019, para. 113.

448. Id.; see also id. at paras. 113–114 (requiring firms to also submit an "Open Architecture" plan, allowing its telephone network to be known to other companies); id. at 1068–69, paras. 223–224 (requiring firms to protect customers' proprietary network information).

449. See Cannon, supra note 426, at 201–02.

450. *Computer III* Further Remand Proceedings, 13 FCC Rcd. 6040, 6051–52, para. 15 (1998) (further notice of proposed rulemaking) (quoting California v. FCC (*California III*), 39 F.3d 919, 928 (9th Cir. 1994)); see also California v. FCC (*California II*), 4 F.3d 1505, 1512 (9th Cir. 1993).

451. See *California III*, 39 F.3d at 928 ("[W]e must consider whether it adequately explains why fully implemented [open network architecture] is no longer regarded as a necessary safeguard against access discrimination after removal of structural separation.").

452. See *Computer III* Further Remand Proceedings, 13 FCC Rcd. at 6044–45, para. 4.

453. See Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C. (2012)). In summary, the Act sought to create competition between telecom companies by requiring that services be unbundled and that providers be interconnected. BOCs were permitted to offer long-distance telephone service to their local customers upon FCC approval. The Act also imposed common carrier requirements on telecom service and empowered the FCC with broad authority to oversee the industry. Shelanski, Adjusting Regulation, supra note 350, at 62–69.

Competition, however, "never arrived."[454] Enforcers permitted waves of consolidation, leading to highly concentrated cable and telecommunications markets.[455] For this reason, policymakers have continued to examine ways to manage the bottleneck power of dominant actors in these markets, most recently in the form of net neutrality.

Notably, the net neutrality policy discussion has occurred within a framework partly established by the Computer Inquiries, which introduced into communications law the conceptual distinction between information and telecommunications. The question of which category internet services fall into has been at the center of the net neutrality debate.

E. *Telecommunications: The Breakup of AT&T*

For much of the twentieth century, the telecommunications industry was intensely regulated through requirements that carrier services, prices, and entry be approved by the FCC and state regulators. The Communications Act of 1934 served as the basic statutory framework guiding the FCC's regulation, which held universal service as a central goal.[456]

In the 1970s AT&T provided local and long-distance phone service, owned a major producer of telephone equipment (Western Electric), and ran a leading research facility (Bell Labs).[457] The Justice Department filed an action against the Bell Systems empire in 1949, alleging that Western Electric had monopolized the manufacturing, sale, and distribution of telephones and other equipment material.[458] In 1974, the government filed a separate action, arguing that AT&T had abused its dominant position in three markets—local exchange, long distance, and equipment—in order to monopolize the entire telecommunications industry, a strategy described as the "'triple-bottleneck' theory."[459] The government's complaint alleged that AT&T had illegally refused to provide competitors with local interconnection services, furnished rivals with inferior maintenance services, and imposed requirements that thwarted the reach of competing local networks.[460]

---

454. Gene Kimmelman et al., The Failure of Competition Under the 1996 Telecommunications Act, 58 Fed. Comm. L.J. 511, 511 (2006).

455. Specifically, the government's approval of the SBC–AT&T and Verizon–MCI mergers marked "the abandonment of the competition model envisioned by the 1996 Act." Id. at 513.

456. Communications Act of 1934, Pub. L. No. 73-416, § 1, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.).

457. Paul W. MacAvoy & Kenneth Robinson, Winning by Losing: The AT&T Settlement and Its Impact on Telecommunications, 1 Yale J. on Reg. 1, 3–4 (1983).

458. United States v. W. Elec. Co., 1956 Trade Cas. (CCH) ¶ 68,246 (D.N.J. 1956).

459. MacAvoy & Robinson, supra note 457, at 14 (quoting The Communications Act of 1978: Hearings on H.R. 13015 Before the Subcomm. on Commc'ns of the H. Comm. on Interstate & Foreign Commerce, 95th Cong. 748 (1978) (statement of John H. Shenefield, Assistant Att'y Gen. for Antitrust)).

460. See United States v. AT&T Co., 524 F. Supp. 1336, 1354–57 (D.D.C. 1981).

In lieu of going to trial, the parties reached a settlement. The agreement required AT&T to divest ownership and control of the BOCs.[461] Premised on the idea that regulators would be unable to stop an integrated monopoly from engaging in predatory anticompetitive conduct in adjacent markets,[462] the settlement was designed to prohibit the companies from combining monopoly and competitive lines of business after divestiture. The Justice Department argued that prohibiting the act of discrimination would be insufficient—the government had to target the underlying incentive to discriminate outright.[463]

Notably, the consent decree combined the breakup requirement with an "equal access" obligation imposed on the independent BOCs. Under this provision, the divested BOCs had to provide unaffiliated long-distance carriers access to the local exchanges that was "equal in type, quality, and price" to that given to AT&T.[464] This obligation was eventually extended to all local-exchange carriers.[465]

The consent decree was administered by Judge Harold Greene for twelve years.[466] Over this time, Judge Greene responded to the parties' requests for modification of the decree, assessing whether the market had sufficiently changed to justify loosening the line-of-business restrictions.[467] The decree remained in place until the passage of the Telecommunications Act.[468]

F. *Common Threads*

Drawing from these separations regimes, a few observations stand out. First, policymakers have applied separations regimes to three sectors: transportation, communications, and banking. Broadly all three have involved

---

461. Joseph D. Kearney, From the Fall of the Bell System to the Telecommunications Act: Regulation Telecommunications Under Judge Greene, 50 Hastings L.J. 1395, 1412 (1999).

462. This premise came to be known as the "Bell Doctrine" or "Baxter's Law." See, e.g., Tim Wu, Intellectual Property, Innovation, and Decentralized Decisions, 92 Va. L. Rev. 123, 139 n.49 (2006) (noting that although Professor William Baxter referred to the premise as the "Bell Doctrine," others refer to it as "Baxter's Law"). In short, Baxter's Law held that:

> [R]egulated monopolies have the incentive and opportunity to monopolize related markets in which their monopolized service is an input, and . . . the most effective solution to this problem is to "quarantine" the regulated monopoly segment of the industry by separating its ownership and control from the ownership and control of firms that operate in potentially competitive segments of the industry.

Paul L. Joskow & Roger G. Noll, The Bell Doctrine: Applications in Telecommunications, Electricity, and Other Network Industries, 51 Stan. L. Rev. 1249, 1249–50 (1999). Notably, Baxter's Law is applicable only in the context of regulated industries.

463. See United States v. AT&T Co., 552 F. Supp. 131, 187 (D.D.C. 1982) ("The restrictions are based upon the assumption that the [BOCs], were they allowed to enter the forbidden markets, would use their monopoly power in an anticompetitive manner.").

464. *AT&T Co.*, 552 F. Supp. at 142.

465. See Kearney & Merrill, supra note 232, at 1351.

466. See Kearney, supra note 461, at 1398–99.

467. See id. at 1417.

468. Id. at 1459.

particular markets and services where a bottleneck facility served as infrastructure or a critical intermediary.[469] Within these categories, we can further distinguish between bottleneck services that are or were essential for the functioning of our economy—such as railroads or banking—and those that constitute an important distribution channel but have not been viewed as essential in the same way.

Second, a majority of the separations were coupled with common carriage rules requiring equal access on equal terms. This was the case with railroads, data processing, and telecommunications, further capturing how structural separations and nondiscrimination rules can function as critical complements in the service of nondiscrimination.

Third, defining the separation may not always be straightforward, especially when dealing with new technologies. With time, the FCC came to see that the initial distinction it had drawn—between data processors and common carriers—was unworkable, prompting the agency to redesign the rule around a distinction between basic and enhanced services instead. This form of learning and reworking is bound to be a part of implementing separations regimes.

Fourth, the efficacy of a separations regime rests intimately on the timing of its implementation. This is true both with regard to its introduction and its repeal. Insofar as it is the existence of a bottleneck that invites the separation, identifying when market conditions have changed such that discrimination or appropriation by the firm is no longer likely to have market-wide effects can help inform if and when a separation should be revoked. The separations implemented through the Computer Inquiries and the *AT&T* remedy both underwent continuous scrutiny by regulators and the judiciary, who regularly evaluated whether the market had become more competitive.[470] And with the exception of banking, the separations regimes discussed above were eliminated once enforcers or lawmakers determined that market developments had created more pathways for distribution, softening the bottleneck's market power. Applying separations requires periodic reassessment that the remedy is still addressing an underlying harm.

Lastly, the separations principle has been applied in different forms. Broadly, two levels of strictness emerge: (1) complete bans (or total separations), which prohibit a company from *any* engagement or involvement,

---

469. See supra sections II.A–.E. Banks may appear to be the exception. But Professor Morgan Ricks notes that recent academic scholarship on banks has improperly focused on their intermediary role of facilitating private transactions, instead of on their monetary role as issuers of funds—a role that gives them "a unique relationship with the state." Morgan Ricks, Money as Infrastructure, 2018 Colum. Bus. L. Rev. 757, 758–59. When one focuses on banks' monetary role, bank regulation "becomes a subfield of public utility and common carrier regulation." Id. at 768–69. Ricks, therefore, argues that "bank regulation might instead embrace infrastructure regulation's logic and follow through on its implications." Id. at 770; see also Rahman, New Utilities, supra note 26, at 1657 ("Finance represents another kind of infrastructural good, a critical service upon which the entire economy depends.").

470. See supra notes 466–468 and accompanying text.

interest, or ownership in particular activity; and (2) partial bans (or functional separations), which permit a company to engage in a particular business activity but prescribe the organizational form it must take—requiring, for example, that the separate business activity be conducted through a separate affiliate. There is no clear pattern as to when lawmakers or regulators opted for one form over the other.

IV. FUNCTIONAL GOALS

This Part explores the policy motivations and functional goals that underlay these structural separations. Although policymakers applied structural limits in a variety of sectors, six justifications recur: (1) eliminating conflicts of interest, (2) preventing cross-financing that would extend existing dominance, (3) preserving system resiliency, (4) promoting diversity, (5) preventing excessive concentration of power, and (6) prioritizing administrability.

Notably, these motivations register in a normatively pluralistic framework: While some are cognizable in terms of welfare economics, others appeal to a broader set of institutional and democratic values. Some goals sound in both registers. This Part reviews these various policy motivations.

A. *Eliminating Conflicts of Interest*

A key policy objective that runs through the separations explored above is the elimination of conflicts of interest. The animating idea is that companies in infrastructure-like sectors that compete with the businesses using their services have an incentive to favor their own goods or services over those owned by rivals. Because these intermediaries comprise a backbone for a broader set of economic or social activity, whether they actually *act* on the incentive and ability to discriminate is secondary—the incentive and ability are deemed a sufficient threat. By forbidding the very structural arrangement that gives rise to the conflict of interest, prophylactic bans safeguard against discrimination.

The goal of eliminating conflicts of interest motivated the implementation and/or enforcement of structural separations in railroads, banking, and computing. As railroads continued to experiment with arrangements that facilitated control over coal, a group of critics argued that the commodities clause should be read as a sweeping structural ban—to prohibit railroads from transporting *any* commodity produced by *any* company in which it held *any* stock. This view was first articulated by Justice John Harlan dissenting in the first commodity clause case to reach the Court.[471] A reading of the act that permitted railroads to affiliate with producers in *any* capacity would, he warned, "enable the transporting railroad company, by one device or another, to defeat altogether the purpose which Congress had in view, which was to divorce, in a real, substantial sense, production and transportation, and thereby to prevent the transporting company from doing injustice to other owners of

471. See United States v. Del. & Hudson Co., 213 U.S. 366, 419 (1909) (Harlan, J., dissenting).

coal."[472] While a majority of the Court refused to go along with this specific interpretation, it rested on the idea that integration created possibilities for abuse, and therefore bans on cross-ownership would help "avoid the tendency to discrimination," which "*necessarily inheres* in the carrying on by a railroad company of the business of manufacturing, mining, producing, or owning, in whole or in part, . . . commodities which are by it transported in interstate commerce."[473] In other words, Justice Harlan wrote, history showed that discrimination "*inevitably* grew up where a railroad company occupied the inconsistent positions of carrier and shipper."[474] Only a clear separation between production and transportation would eliminate this risk of discrimination.

Similarly, the structural separation in banking was driven by the desire to prevent conflicts of interest that could bias how banks make loans or extend credit. Owning or even affiliating with a commercial entity could incentivize banks to make lending decisions with an eye to the effects on their own commercial entities.[475] By interfering with the allocation of credit, this dynamic could threaten to distort not just competition in any given market but the economy as a whole.[476]

At root, the concern about biased lending echoes the antitrust fear about foreclosure. Both focus on how an integrated business may use its integrated structure to undermine or discriminate against rivals. The concern is more acute in the context of banking given the critical role financial institutions play in providing access to credit, the lifeblood of the economy.

The FCC echoed concerns about conflicts of interest in the Computer Inquiries. As the telephone companies expanded into the nascent computing market—thereby competing with the data-processing firms dependent on them[477]—the FCC worried about "even the most subtle preferences a common carrier might give its data processing subsidiary."[478] In its tentative decision first considering the structural regime, the Commission observed that the

---

472. Id.

473. Id. at 404 (majority opinion) (emphasis added).

474. United States v. Reading Co., 253 U.S. 26, 61 (1920) (emphasis added).

475. See, e.g., S. Rep. No. 100-19, at 8 (1987), as reprinted in 1987 U.S.C.C.A.N. 489, 498 (noting that commercial ownership by banks "raises the risk that the banks' credit decisions will be based not on economic merit but on the business strategies of their corporate parents").

476. J.P. Morgan running a copper business, for instance, could skew its lending decisions in a couple of ways. The bank could discriminate against competing copper companies, choosing to extend credit at unfavorable rates or declining to lend at all. It could also discriminate among suppliers or buyers of its copper—conditioning credit on favorable treatment for its commercial affiliate. Aggregated across millions of lending decisions, this biased approach—penalizing competing copper companies and pressuring borrowers into doing business with J.P. Morgan's own copper dealer—could determine not only the fate of any single copper company but the trajectory of the copper sector as a whole.

477. See *Computer II*, 77 F.C.C.2d 384, 389–90, para. 15 (1980) (final decision) (explaining that a major goal of the Computer Inquiries was to address "whether communications common carriers should be permitted to market data processing services").

478. Steve Bickerstaff, Shackles on the Giant: How the Federal Government Created Microsoft, Personal Computers, and the Internet, 78 Tex. L. Rev. 1, 17 (1999).

primary dangers of allowing common carriers to integrate into data processing "relate primarily to the alleged ability of common carriers to favor their own data processing activities by discriminatory services, cross-subsidization, improper pricing of common carrier services, and related anticompetitive practices and activities."[479]

Notably, the FCC acknowledged that permitting carriers to use excess capacity for data processing might yield efficiencies that could lower costs.[480] But the agency maintained that "the potential abuses inherent in operations of this nature outweigh whatever benefits might be achieved."[481] Moreover, the FCC argued that permitting carriers to integrate would distort the market by enabling a firm to succeed based on existing dominance rather than business-specific talent.[482]

B. *Preventing Protected Profits from Financing Entry into New Markets*

Another concern that recurs as a functional justification is the desire to prevent companies from using protected profits to finance entry into new lines of business—a tactic that was deemed anticompetitive. This concern was especially heightened in the context of banking and telecommunications, as officials worried that firms would use their regulated services to finance their unregulated businesses.[483]

---

479. *Computer I*, 28 F.C.C.2d 291, 301–02, para. 33 (1970) (tentative decision). Reviewing the structural separation, the U.S. District Court for the District of Columbia echoed the FCC's concerns, noting that:

> [T]he ability for abuse exists as does the incentive, of that there can . . . be no doubt. . . . Among the more obvious means of anticompetitive action in this regard are increases in the rates for those switched and private line services upon which Regional Company competitors depend while lower rates are maintained for Regional Company network services; manipulation of the quality of access lines; impairment of the speed, quality, and efficiency of dedicated private lines used by competitors; development of new information services to take advantage of planned, but not yet publicly known, changes in the underlying network; and use for Regional Company benefit of the knowledge of the design, nature, geographic coverage, and traffic patterns of competitive information service providers.

United States v. W. Elec. Co., 673 F. Supp. 525, 566 (D.D.C. 1987).

480. See *Computer I*, 28 F.C.C.2d 267, 271, para. 13 (1971) (final decision and order).

481. Id.

482. The Commission noted in its tentative decision that "[t]he factors which mark the difference between service bureau success or failure are imaginative innovation, quality programming, and useful service features, rather than the size of the staff or the computing installation." *Computer I*, 28 F.C.C.2d at 298, para. 21 (tentative decision). In its final decision and order, the Commission also stated its belief "that [its] restrictions herein respecting corporate arrangements are neither onerous nor burdensome but reflect, rather, the market conditions confronted by those 800 or more noncarrier-related firms with whom carrier data affiliates will be competing." *Computer I*, 28 F.C.C.2d at 272, para. 16 (final decision and order).

483. Separations policies were applied in the context of regulated monopolies to prevent three anticompetitive practices: (1) the monopolist's use of profits earned from regulated markets to engage in predatory pricing in the unregulated markets; (2) the monopolist's control of the supply of competitors (assuming the two markets are related); and (3) the monopolist's

The separation of banking and commerce, for example, was seen as a way to keep banks from leveraging a government-granted advantage into other lines of business.[484] Some accounts view this as a foundational reason that England first instituted the separation. As the British government had granted the Bank of England a corporate charter, separation was a "protection against whatever advantages the special corporate charter implied and whatever advantages the Bank might obtain in the future."[485] Keeping banks from entering commerce would prevent a government-sponsored entity from constraining opportunities for private entrepreneurs. In other words, separation was a "protection against a firm affiliated with the government."[486]

In computing, the FCC wanted to prevent regulated telephone monopolies from subsidizing their data-processing entities, which would have given them an edge over independent data processors.[487] Because data processors depended on the carriers, permitting carriers to enter computing would mean the carrier's data-processing division would receive an "implicit subsidy" from its competitors.[488] This would lead to "unfairly and artificially low prices in the data processing market for the carrier's computer services."[489] And because the monopoly had its long-run rate of return effectively guaranteed, it had latitude to engage in predatory pricing.[490]

Again, this cross-financing was viewed as anticompetitive, as it would permit the monopoly to leverage its government-protected advantage against firms in a separate market. The FCC wanted to "prevent any arbitrary

---

assignment of all joint costs to the regulated product, charging a higher price in the regulated market. See W. Kip Viscusi et al., Economics of Regulation and Antitrust 546–49 (4th ed. 2005) (highlighting the anticompetitive practices that "might result from allowing a regulated monopolist to compete against unregulated firms" and describing how "[t]he benefits of separation rest in preventing such practices from taking place").

484. Professors Bob Hockett and Saule Omarova explain how banking has always functioned as a form of public franchise, built upon the full faith and credit of the U.S. government. See Robert C. Hockett & Saule T. Omarova, "Special," Vestigial, or Visionary? What Bank Regulation Tells Us About the Corporation—and Vice Versa, 39 Seattle U. L. Rev. 453, 461 (2016).

485. Shull, supra note 391, at 274.

486. Id. Some scholars argue that this aversion to "crony capitalism" and "trade monopolists" led in part to the American Revolution and played a key role in foundational debates about the federally incorporated Bank of the United States, the scope of the Contracts Clause, and the Fourteenth Amendment. See Steven G. Calabresi & Larissa C. Leibowitz, Monopolies and the Constitution: A History of Crony Capitalism, 36 Harv. J.L. & Pub. Pol'y 983, 984–88 (2013). A version of this same concern might focus on the implicit subsidy that large U.S. banks enjoy. In 2014 the International Monetary Fund (IMF) documented that big banks benefit from "implicit public subsidies created by the expectation that the government will support them if they are in financial trouble." The IMF estimated that "global systemically important banks" enjoyed a $70 billion subsidy in the United States and up to $300 billion in the euro area. IMF Survey: Big Banks Benefit from Government Subsidies, IMF (Mar. 31, 2014), http://www.imf.org/en/News/Articles/
2015/09/28/04/53/sopol033114a [https://perma.cc/W973-6JCZ].

487. See supra notes 431–436 and accompanying text.

488. Note on FCC Computer Inquiry, supra note 429, at 190.

489. Id.

490. Id.

manipulation in the allocation of revenues and expenses between a carrier's regulated and unregulated service offerings."[491] Specifically, the FCC worried that a carrier could charge inflated prices to its customers and use these revenues to finance its data-processing unit, which could underprice competitors in the data-processing market.[492] This concern applied even in the context of smaller carriers, which would still have "the incentive and opportunity to take advantage of their monopoly control of the transmission capacity, and to act in anticompetitive ways."[493]

The FCC's desire to prevent the affiliate from enjoying *any* residual benefits from the monopoly led it to prohibit affiliates from sharing even names or symbols with the common carrier.[494] Branding the affiliate as an extension of the common carrier would produce the "same coercive effect" as if the carrier were soliciting sales on behalf of its data-processing business.[495]

Preventing cross-financing was treated as a tool to enhance competition in the data-processing market. Allowing exclusive transactions between a carrier and its affiliate would "substantially impact the competitive market in which hundreds of small competing service bureau firms would be unable to obtain and retain the patronage of so significant a data processing customer."[496] This is one reason the FCC required carriers to provide basic services to all other enhanced services on the same terms and conditions—effectively combining a structural separation with a nondiscrimination regime.

C. *Preserving System Resiliency*

Another justification that recurs is promoting the resiliency of systems. Because several of the entities subject to structural separations serve an "infrastructural" role—structuring access to markets or to an essential good or service—the public has a strong interest in maintaining their stability and shielding them from disruption.[497] Crashes that cripple these infrastructural services can have an outsized effect on economic activity, and involvement in multiple lines of business can increase the likelihood of system crashes. For this reason, policymakers treated strict limits on entry and exit as one way to

---

491. *Computer I*, 28 F.C.C.2d 267, 273, para. 20 (1970) (final decision and order).

492. Id.

493. Cannon, supra note 426, at 194.

494. *Computer I*, 28 F.C.C.2d at 272, para. 18 (final decision and order).

495. Id.

496. Id. at 273, para. 19.

497. For a definition of "infrastructural," see Rahman, New Utilities, supra note 26, at 1640–44. It's also worth noting that the definition is contested. Even investors lack any single definition of "infrastructure." Ryan Dezember & Miriam Gottfried, What Do Laundry Machines and Roads Have in Common? To Investors, They're Infrastructure, Wall St. J. (Mar. 5, 2018), https://www.wsj.com/articles/what-do-laundry-machines-and-roads-have-in-common-to-investors-theyre-infrastructure-1520282663 (on file with the *Columbia Law Review*) ("Blackstone notes that the term infrastructure is open to interpretation: 'There is no generally accepted definition of infrastructure.'").

shield critical services from undue risk.[498] Structural separations in banking and telephony, too, were partly justified on grounds of promoting system stability.[499]

Precisely because banking services constitute a critical good, ensuring the soundness and stability of banking is a central goal of banking policy. Lawmakers and regulators have argued that preventing banks from expanding into commercial activities may help insulate banks from the vagaries of other sectors.[500] This line of argument is premised on the idea that exposing banks to manufacturing, physical trading, or other commercial activities "increases the vulnerability of the banking and payments systems, the federal deposit insurance fund, and thereby the broader economy."[501] A question frequently raised during the 2013 debates around banks' expansion into physical commodity trading was: What would happen if Morgan Stanley repeated the BP oil spill? Would taxpayers be on the line for the $61.2 billion in damages? In this way, a structural separation helps eliminate the risk that instability or disruption in commercial markets could necessitate a financial bailout.[502]

To be sure, not all commercial activities are inherently more risky than financial activity—and, some might argue, expanding into these spheres may help banks *diversify* risk. That said, it is true that some commercial activities—like drilling oil or mining—pose particularly expensive risks to which federally insured depository institutions should not be exposed.[503]

Concerns about system stability and resiliency also informed the FCC's Computer Inquiries. The carriers argued that, in order to promote efficiency, they should be permitted to use excess capacity for data processing.[504] The

---

498. See Richard J. Pierce, Jr. & Ernest Gellhorn, Regulated Industries in a Nutshell 251–74 (4th ed. 1999).

499. See, e.g., Randall S. Kroszner & Raghuram G. Rajan, Is the Glass-Steagall Act Justified? A Study of the U.S. Experience with Universal Banking Before 1933, 84 Am. Econ. Rev. 810, 810 (1994) ("The driving force behind the Act was Senator Carter Glass, who strongly believed that direct commercial-bank involvement with corporate securities was detrimental to the stability of the financial system.").

500. See, e.g., David Sheppard & Alexandra Alper, Insight: As Banks Deepen Commodity Deals, Volcker Test Likely, Reuters (July 3, 2012), https://www.reuters.com/article/us-commodities-forwards-banks/insight-as-banks-deepen-commodity-deals-volcker-test-likely-idUSBRE86206420120703 [https://perma.cc/42R9-J7XJ] (quoting senators as decrying bank expansion into commodities-related businesses due to the risk potential); Editorial, The Value of the Volcker Rule, Wash. Post. (Oct. 28, 2011), https://www.washingtonpost.com/opinions/the-value-of-the-volcker-rule/2011/10/18/gIQATZhUQM_story.html (on file with the *Columbia Law Review*) (noting arguments by Paul Volcker, Chairman of the Federal Reserve at the time, in favor of requiring banks to separate investment banking practices from traditional commercial banking practices).

501. Omarova, supra note 410, at 275–76.

502. See Nathaniel Popper & Peter Eavis, Senate Report Finds Goldman and JPMorgan Can Influence Commodities, N.Y Times: Dealbook (Nov. 19, 2014), https://dealbook.nytimes.com/2014/11/19/senate-report-criticizes-goldman-and-jpmorgan-over-their-roles-in-commodities-market/ (on file with the *Columbia Law Review*).

503. See id. at 317–18 (noting that "[g]lobal energy prices are notoriously volatile").

504. See *Computer I*, 28 F.C.C.2d 267, 271, para. 13 (1970) (final decision and order).

Commission stated, first, that "the potential abuses inherent" in the system far outweighed any purported efficiencies,[505] and, second, the carriers should have a "'back-up' system" that "should be designed to meet foreseeable breakdowns of equipment dedicated to public service" and "should be available instantly for that purpose without the conflicting claims of other users."[506] In other words, the FCC privileged redundancy over efficiency, recognizing that the former would serve the public by helping to ensure the stability of communications services and networks. Although expanding into data processing wouldn't necessarily heighten the risk of a crash, keeping that capacity for backup would enable the system to absorb any shocks, helping promote resiliency.

D. *Promoting Diversity*

By creating conditions that invite greater competition among producers, structural bans can promote diversity in the goods and services produced. The history of the media sector shows that mandating a separation between production and distribution can help create an open market for content.[507]

A key reason the FCC issued the fin-syn rules was to promote media diversity. One effect of the networks' vertical control was that they effectively controlled the production process of most programming, "from idea through exhibition."[508] Their programming decisions, in turn, were driven by advertising profits. As a result, "programs were produced on the basis of 'formulas' that were pre-approved by the three networks and their advertisers, such that the subject matter would satisfy tested commercial patterns."[509] The networks' grip on production, coupled with their commercial priorities, dramatically limited the range of programming that they would run. Lacking both the financial support of the networks as well as national exposure, independent producers languished.[510] The FCC worried that the networks' dominance was sapping program diversity, limiting the shows and voices that Americans could access.[511]

---

505. Id.

506. Id.

507. See Herskovitz, supra note 419, at 179–81 (arguing that FCC-mandated separation in media created an environment in which, "for the first time, independent producers were bargaining from a position of relative strength").

508. Id. at 186 (internal quotation marks omitted) (quoting Competition & Responsibility in Network Television Broad., 23 F.C.C.2d 382, 389, para. 11 (1970) (report and order)).

509. Id. at 187.

510. Id. at 188–89.

511. See id. at 179–80 (noting that the impetus behind fin-syn was to "foster a more competitive and diverse programming climate"). Available data validate the worry: From 1957 to 1968, the percentage of prime-time network programming provided by independent producers had fallen from 33% to 4%. Douglas Ginsburg et al., Regulation of the Electronic Mass Media 266 (2d ed. 1991).

For this reason, the FCC structured its rules with diversity as a primary goal.[512] Key to achieving greater variety in programming was restructuring the networks' incentives and restricting their ability to steer content. On this metric, the fin-syn rules worked: Between 1970 and 1990, the number of independent television stations increased from 65 to 340.[513] The Big Three networks' aggregate share of nationwide primetime audience over this same period, meanwhile, declined from 90% to nearly 62%.[514]

Safeguarding diversity of information also motivated Judge Harold Greene to modify the government's consent decree with AT&T.[515] The decree proposed by the Justice Department would have permitted the new AT&T—having divested local carriers—to provide electronic publishing services.[516] Reviewing the provision, Judge Greene held that First Amendment values required that AT&T be blocked from entering this market.[517]

Judge Greene's primary concern was that AT&T would use its power in the interexchange market to undermine competing electronic publishers. He identified a set of tactics that the corporation could use to discriminate against rivals.[518] For example, he explained, AT&T could use its control over the network to prioritize traffic from its own publishing operations, to develop technology that favored its own operations over those of the industry at large, or to discriminate against competitors when providing needed maintenance on their lines.[519]

Judge Greene acknowledged the Justice Department's likely argument—namely, that market dynamics would limit AT&T's ability to discriminate.[520] But he stated that "the peculiar characteristics of the electronic publishing market" invited particular caution.[521] Noting that information and news were "especially sensitive" to even small delays, and that publishers would "have no realistic alternative transmission system," he concluded that "AT&T's entry into the electronic publishing market poses a substantial danger to First

512. Specifically, the agency sought to promote diversity across three different dimensions: source diversity, outlet diversity, and program diversity. See Herskovitz, supra note 419, at 200–06 (discussing the various results of fin-syn in the television marketplace).

513. Christian, supra note 415, at 109.

514. Id. The FCC's repeal of fin-syn was controversial. On the one hand, industry groups and some public advocates stressed that the advent of new technologies had injected fresh competition in the media marketplace, dissolving the networks' grip. Others held that the networks still possessed the ability to steer and manipulate programming at the expense of source and outlet diversity. See Herskovitz, supra note 419, at 200 ("Commentators have taken the position that the repeal of the rules was a prudent judgment . . . point[ing] to the prolification of broadcast outlets such as cable, VCRs, and direct broadcasting . . . . They point to these as evidence of competition in the industry and an increasing supply of diverse programming." (footnote omitted)); Id. at 200–01.

515. United States v. AT&T Co., 552 F. Supp. 131, 181 (D.D.C. 1982).

516. Id. at 180.

517. Id. at 181–83.

518. Id. at 181.

519. Id.

520. Id. at 182.

521. Id.

Amendment values."[522] Judge Greene required that the consent decree be modified to prohibit AT&T from entering electronic publishing for seven years, with the prospect of extension if the court determined that threats remained.[523]

Abandoning the principle of structurally separating production and distribution has enabled widespread integration across media markets—potentially at the expense of media diversity. Critics of the Comcast–NBC merger, for example, warned that the tie-up would incentivize Comcast to privilege NBC programming[524]—and evidence suggests that Comcast has, in fact, discriminated against rival content.[525] The recent vertical tie-up of Time Warner and AT&T[526] poses some of the same hazards—including, public advocates predict, less media diversity.[527] Weeks after the D.C. Circuit approved the deal, AT&T threatened to drop rival programming, prompting allegations that the merged firm was using its "newfound market dominance" as "leverage to drive consumers to the content it owns."[528]

E. *Preventing Excessive Concentration of Power and Control*

By preventing certain forms of centralized control, structural separations can help safeguard against the concentration of power. The antimonopoly movement and the foundational antitrust laws were partly animated by a recognition that tyranny in our commercial spheres would preclude true democracy and liberty in our political sphere.[529] Structural separations were

---

522. Id. at 182–83.

523. Id. at 225. The U.S. Court of Appeals for the D.C. Circuit vacated Judge Greene's prohibition against a BOC's provision of information services, on the basis that BOCs could not be prevented from entering a market absent specific evidence that they had engaged in anticompetitive abuses in that market. United States v. W. Elec. Co., 894 F.2d 430, 436–38 (D.C. Cir. 1990).

524. See Kim Hart, Comcast-NBC Merger Conditions Expire, Raising Anti-Competitive Fears, Axios (Jan. 22, 2018), https://www.axios.com/comcast-nbm-1516393866-a394d1c7-abc5-4f51-879e-3fcab1c0de89.html [https://perma.cc/H2AY-F7AB] (citing concerns of Senator Richard Blumenthal and then-FCC Commissioner Mignon Clyburn over the prospect of Comcast owning the distribution of both content and programming).

525. See Jasmin Melvin, U.S. FCC Sides with Bloomberg over Comcast Dispute, Reuters (May 2, 2012), http://www.reuters.com/article/fcc-comcast-bloomberg-idUSL1E8G2N8C20120502 [https://perma.cc/9K3D-9CR7] (describing an FCC decision finding that Comcast had violated a "neighborhooding" requirement by not placing Bloomberg's financial news channel near other news channels in its lineup).

526. The District Court for the District of Columbia approved the merger in June 2018. See United States v. AT&T Inc., 310 F. Supp. 3d 161, 165 (D.D.C. 2018).

527. See, e.g., Shiva Stella, Public Knowledge President to Testify on AT&T/Time Warner Merger, Pub. Knowledge (Dec. 6, 2016), https://www.publicknowledge.org/press-release/public-knowledge-president-to-testify-on-att-time-warner-merger [https://perma.cc/FVA6-MHPT].

528. Sara Fischer, In AT&T and Viacom Spat, Cable Customers Lose Out, Axios (Mar. 22, 2019), https://www.axios.com/att-viacom-directv-blackout-cable-tv-dispute-3945f9c1-9e7f-4711-b5f7-d0d8a3d20d02.html [https://perma.cc/2HVS-F4YJ].

529. See Zephyr Teachout & Lina Khan, Market Structure and Political Law: A Taxonomy of Power, 9 Duke. J. Const. L. & Pub. Pol'y 37, 61 (2014) ("[E]xploration of the Sherman Act's

seen as a tool in this antimonopoly toolbox. Perhaps due to the outsized power that a financial oligarchy can wield—and the trove of findings by the Pujo Committee showing how a handful of financiers had seized control over entire sectors of the economy[530]—preventing excessive concentration featured as a prominent justification in debates on banking law through the mid-twentieth century.[531]

On some accounts, all bank holding company regulation in the United States has had this antimonopoly goal as its focus—both to prevent "the unrestrained concentration of banking resources under the control of a single organization" and "to prevent undue concentration of economic power that Congress perceived may result when banking and nonbanking enterprises combine under the same corporate umbrella."[532] The BHCA follows this antimonopoly tradition, and its passage was in part the product of effective lobbying by small independent and community banks.[533] Embedded in the separation of banking and commerce is a preference for small, local business enterprise as a unit of economic activity.[534]

How would banks' foray into commercial activities risk concentrating excessive power, rather than exhibiting bigness per se? One factor is control. If the same organizations that control access to money also control access to commercial products and services, banking experts worry that the arrangement would hand outsized decision-making power to a few. This concern is heightened when the products and services are of an essential nature—such as commodity inputs and raw materials like copper, grain, and energy—and when the controlling banks hold dominant positions.[535]

If one worry about big banks steering both credit and commerce is outsized economic control, the other is excessive political influence. The ways that corporate actors can translate economic power into political influence are legion.[536] If history suggests that banks and finance interests have enjoyed

---

intellectual antecedents shows that for Senator Sherman and the Act's congressional supporters, economic and political freedoms were seen as part of a piece.").

530. See H.R. Rep. No. 62-1593, at 133 (1913); see also Louis D. Brandeis, Other People's Money and How the Bankers Use It 2–6 (1914) (describing the Pujo Committee report and arguing that the outsized power of the financial oligarchy—driven by investment bankers in particular—poses a danger to political liberty).

531. See Omarova, supra note 410, at 276–77 (noting the BHCA's original focus as an "antitrust, anti-monopoly law").

532. Melanie L. Fein, Federal Bank Holding Company Law § 7.01[1] (3d ed. 2018).

533. Omarova, supra note 410, at 277.

534. See id.

535. This potential hazard recently came to the surface around 2013, when the public learned that some of our biggest banks—Goldman Sachs, J.P. Morgan, and Morgan Stanley—had also morphed into some of the biggest merchants of physical goods, supplying crude oil, storing aluminum, and running electricity plants. See id. at 266–67 (describing these banks' ventures into commodity industries); Goldman Sachs's Aluminum Pile, supra note 408 (arguing that policymakers should investigate financial institutions' commodities-driven profits).

536. See Simon Johnson & James Kwak, 13 Bankers: The Wall Street Takeover and the Next Financial Meltdown 3–13 (2011) ("The Wall Street banks are the new American oligarchy—a

political influence by virtue of their influence over the American economy, then prohibiting banks from acquiring significant equity in American industry remains one safeguard against their amassing greater political power.

F. *Prioritizing Administrability*

A final functional justification for structural separations is that they are highly administrable. Issuing outright bans obviates the need to engage in lengthy rule-of-reason type analysis; structural limits prescribe rules instead of standards. Structural separations are sometimes criticized for being far-reaching, crude, and overly broad, prohibiting benign as well as pernicious activity.[537] This criticism is fair, given that rules are "by nature both over- and under-inclusive."[538] They accept some degree of error in return for clarity and predictability.

In at least two instances, public officials introduced structural regimes by citing their administrability, noting the limits of the government's capacity to consistently detect discrete acts of wrongdoing. The FCC, for example, stressed its inability to "monitor carefully" the types of activities it had prohibited, "since even the injured party may not be aware of them."[539] The Commission observed that "subtle forms of favoritism" are "numerous and difficult to detect," and that it was unlikely that the agency would "be prompt in cracking down on discovered abuses."[540] Relying on the agency to track individual acts of injury would risk extensive harm to competition. Structural bans, the agency explained, could also aid "the deterrence of foreseeable abuse."[541]

Members of Congress cited some of these same factors when constructing the BHCA. Lawmakers acknowledged that not *all* banks that expanded into commerce would discriminate or otherwise abuse their power.[542] But short of flagrant abuses, "subtle bias" might creep in, and it would be "quite unrealistic

---

group that gains political power because of its economic power, and then uses that political power for its own benefit."); Teachout & Khan, supra note 529, at 37–38 (explaining how "decentralized economic power and democratic self-government are deeply intertwined" and arguing that market structure is "innately political"); see also Johnson & Kwak, supra, 88–94 (noting that the "dismantling of the regulatory system" that occurred in the 1990s and 2000s coincided with increasing political donations from the financial sector and Wall Street bankers taking on "major positions in the government during the Clinton and George W. Bush administrations"); James Kwak, Cultural Capture and the Financial Crisis, *in* Preventing Regulatory Capture: Special Interest Influence and How to Limit It 71, 79–81 (Daniel Carpenter & David A. Moss eds., 2014) (describing the phenomenon of "cultural capture," a process whereby regulators systematically favor regulated industries whose members share a common identity with the regulators, are in the regulators' social networks, or are generally perceived as high-status individuals).

537. See infra Part V.

538. Jessica Bulman-Pozen & David E. Pozen, Uncivil Obedience, 115 Colum. L. Rev. 809, 843 (2015).

539. Note on FCC Computer Inquiry, supra note 429, at 200.

540. Id.

541. *Computer I*, 28 F.C.C.2d 267, 273, para. 20 (1971) (final decision and order).

542. See Omarova, supra note 410, at 277–78 (describing exemptions from the general statutory restrictions separating banking and commerce).

to expect [banking regulators] to monitor and detect" these less overt forms of discriminatory lending.[543]

G. *Shared Features Across Justifications*

As explored above, six primary justifications recur across the structural separations reviewed: (1) eliminating conflicts of interest, (2) preventing dominant firms from using protected profits to enter new markets, (3) preserving system resiliency, (4) promoting diversity, (5) limiting the concentration of power, and (6) prioritizing administrability.

Several justifications share features, even as they draw on different values. First, these goals generally seek to preserve the integrity of a process rather than achieve a specific market outcome. Eliminating conflicts of interest and preventing use of protected profits to finance entry, for example, target purported distortions of market competition; both seek to curb a firm's ability to harness existing market power. While the rhetoric surrounding these two justifications occasionally draws on notions of fairness, the substantive justifications also ring soundly in welfare terms, given that preventing dominant firms from harnessing existing advantages at the expense of new firms can promote dynamic efficiency. Preserving system resiliency, too, can be viewed as a welfare-based goal, insofar as ensuring greater reliability of core infrastructure is likely to facilitate greater economic activity.

Several of the policy goals, however, can instead be understood as appealing to a broader set of democratic and institutionalist values.[544] Preserving the system resiliency of essential services, for example, also draws on a tradition concerned with facilitating broad access to critical resources and restricting the arbitrary power that providers of essential services can exercise. Promoting diversity in production and preventing the excessive concentration of private power, meanwhile, are informed by a foundational recognition of the connection between economic structure and political outcomes. Drawing on the republican insight that domination is wrongful "even if the empowered party never affirmatively interferes with the dependent's party choices," structural separations target the *source* of the power, rather than its exercise.[545]

---

543. Jonathan Brown, The Separation of Banking and Commerce, GIS for Equitable and Sustainable Communities, http://www.public-gis.org/reports/sbc.html [https://perma.cc/G5LG-F3X8] (last visited Oct. 20, 2018).

544. Leading contemporary republican thinkers describe domination as subjection to another's arbitrary power. See, e.g., Philip Pettit, Republican Freedom: Three Axioms, Four Theorems, *in* Republicanism and Political Theory 102, 102 (Cécile Laborde & John Maynor eds., 2008) (reformulating "the republican conception of freedom as non-domination" and, in doing so, using the "notion of being subject to the alien control of others . . . to represent the idea of domination").

545. Evan J. Criddle, Liberty in Loyalty: A Republican Theory of Fiduciary Law, 95 Tex. L. Rev. 993, 1003 (2017) ("The mere fact that the empowered party has the *capacity* for arbitrary interference underscores the dependent party's vulnerability, impressing upon the dependent party's mind the need to remain within the power holder's good graces.").

V. TOWARD A GENERAL FRAMEWORK FOR SEPARATING PLATFORMS AND COMMERCE

The competition issues posed by dominant digital platforms have emerged against a doctrinal and institutional backdrop that seems particularly ill-equipped to handle them. The enfeebling of antitrust, coupled with the shift away from direct regulation of network industries, has permitted businesses that enjoy dominant positions as key infrastructure to integrate in ways that threaten to undermine competition. Yet even prominent proponents of deregulation have championed strong antitrust enforcement, including limits on vertical mergers.[546]

The debate around how to tackle the power of dominant tech platforms is in its early stages. Recognizing that these entities play critical gatekeeper roles can help illuminate legal regimes that have been used to address analogous challenges in the past. While structural separations were a mainstay in a previous era, their role in structuring open markets has been largely abandoned.[547]

This Part examines whether integration by dominant platforms gives rise to the sort of harm previously addressed through separations, offers a rough sketch of what a separations framework for digital intermediaries might look like, and identifies the likely challenges and unresolved questions. Ultimately, any separations proposal will require a case-by-case analysis of the relevant market that the platform dominates, the types of network effects and entry barriers that suggest the platform's market power may be durable, and the potential costs of implementing a separation. Several questions that this Part only briefly engages—such as how to define what constitutes a platform, how to assess the contours of the platform, and how to scope structural separations—invite deeper study.

A. *Substantive Case*

1. *Innovation Concerns.* — Reports document that dominant digital platforms are using their integrated structure to discriminate against rivals and appropriate their competitively significant business information.[548] If this

546. See, e.g., Stephen Breyer, Regulation and Its Reform 158 (1982) ("[T]he antitrust laws rest upon the assumption that a workably competitive marketplace will achieve a more efficient allocation of resources, greater efficiency in production, and increased innovation . . . . Where this assumption holds true, antitrust would ordinarily seem the appropriate form [of] government intervention."); 2 Alfred E. Kahn, The Economics of Regulation 115 (1971) ("The only government planning required is of the antitrust kind—directed at preserving the competitive market *mechanism*—and related efforts to make that mechanism work as well as possible."); Breyer, Analyzing Regulatory Failure, supra note 249, at 557 ("Where predatory pricing might exist, it can be dealt with through application of the antitrust laws."); Alfred E. Kahn, Deregulation: Looking Backward and Looking Forward, 7 Yale J. on Reg. 325, 348 (1990) ("[T]he government clearly has neglected responsibilities of which it was never the intention of deregulation to relieve it. These include . . . vigorous enforcement of the antitrust laws . . . .").

547. See supra section II.B.

548. See supra sections I.A–.D.

dynamic depresses the incentive to innovate—as studies suggest it does[549]—then this cost of digital platform integration is worth taking seriously. While standard economic theory states that only under certain exceptions will dominant platforms have the incentive and ability to discriminate against complementors, digital markets characterized by network externalities help create the conditions under which platforms are likely to discriminate.[550] Moreover, because dominant digital platforms passively capture highly precise and nuanced data on their business customers—information that is more valuable by virtue of being more sophisticated[551]—both the risk and cost of information appropriation is heightened in digital markets.

Concerns about information exploitation are not new. In 1971, when the FCC was considering whether its "maximum separation" regime should prohibit involvement by carriers in data processing entirely (or should require instead that their data-processing services be run as an independent affiliate),[552] it noted that an integrated carrier could potentially misappropriate information against processor rivals.[553] Data processors worried that integrated carriers would be able to collect their sensitive business information to exploit against them as rivals in data processing. The FCC concluded that this risk of misappropriation was low.[554] Its final decision stated that that the majority of independent data processors would likely use the Bell System for communication services,[555] and since Bell was forbidden from operating in unregulated markets (including data processing) altogether, there would be no risk of misappropriation of information by a rival.[556] Still, the FCC recognized the potential threat and noted it would "consider any attempt on the part of a carrier to secure and use such information for the benefit of its data processing affiliate as a serious breach of the policy established herein."[557]

2. *Broader Concerns.* — As reviewed in Part IV, separations have been motivated by a host of functional goals, some of which fit squarely within a welfarist frame, while others appeal to a set of institutional and democratic values. Recalling these broader concerns that animated laws and regulations effecting separations helps bring into focus the range of factors at stake when

549. See, e.g., Zhu, supra note 204, at 24–26.

550. See infra Appendix.

551. See supra sections I.A–.D.

552. See *Computer I*, 28 F.C.C.2d 267, 269–70, paras. 10–11 (1971) (final decision and order).

553. See id. at 281–82, para. 39. The Commission's final decision stated, "[T]he fear is expressed that provision to the carrier of detailed information regarding a competitive offering is, in essence, provision of such information to the carrier's data affiliate." Id.

554. Id.

555. See id. ("[T]he majority of such non-affiliated firms will doubtless turn to companies of the Bell System for communication services and facilities since the latter provide the greater share of such services.").

556. Id.

557. Id. at 282, para. 39.

dealing with a dominant intermediary. Below I briefly review how these functional goals do or do not resonate in the context of digital platforms.

a. *Extending Dominance Through Cross-Financing.* — As described above, structural separations imposed on banks and telecommunications carriers were partly motivated by a desire to prevent cross-financing. Lawmakers and regulators worried that firms whose dominance stemmed from government-granted privileges would use that cushion to advantage new lines of business.[558] In particular, they worried that companies would use their regulated monopoly businesses to finance their unregulated businesses, thus gaining a competitive edge over rivals.[559]

One way in which this could occur is if a firm shifted the costs of supplying the unregulated market to the regulated sector. The regulator—hypothetically unable to detect that the higher costs should be attributed to a distinct market—would then raise the revenue requirement that ratepayers of the regulated product would have to cover.[560] Effectively forcing consumers of the firm's regulated service to finance its entry into the unregulated market would, in turn, undermine competition by discouraging potential rivals from entering the unregulated market.[561]

Because digital platforms are unregulated, they cannot use regulated rates to finance new ventures. To the degree that it is the *regulated* nature of the subsidizing rates—namely, the fact that these rates are set by the government in a market where customers lack real choice—then digital platforms do not raise analogous concerns. If, instead, the concern is responding to dominant firms using supracompetitive profits to finance entry in an array of other markets, then the platform fact pattern becomes relevant.[562]

Since dominant platforms report earnings and revenue at a highly generalized level, without breaking revenues and profits down to specific lines of business, we can mostly only speculate about the degree to which these firms are cross-financing. For example, Google's operating margins over the last decade have hovered between 22% and 35%,[563] margins that would qualify

---

558. See supra section IV.B.

559. See supra notes 484–493 and accompanying text.

560. Timothy J. Brennan, Cross-Subsidization and Cost Misallocation by Regulated Monopolists, 2 J. Reg. Econ. 37, 37 (1990).

561. See id. ("[T]he ability to set marginal costs low through cross-subsidization can discourage potential entrants from entering a market, even if the pre-entry price is above their average cost . . . .").

562. Antitrust experts previously have cited cross-financing as enabling predatory conduct. See Remedies Brief of Amici Curiae Robert E. Litan et al. at 54, United States v. Microsoft Corp., 87 F. Supp. 2d 30 (D.D.C. 2000) (No. 98-1232), https://www.brookings.edu/wp-content/uploads/2016/06/20000428.pdf [https://perma.cc/PMY6-XSVW] ("Microsoft's deep pockets have financed its predatory actions. In whatever structure the Court finally decides, therefore, care should be taken to ensure that the vast cash resources of the company are not lodged in an entity that can use them for anticompetitive purposes . . . .").

563. Alphabet Inc (NAS:GOOG) Operating Margin %, Guru Focus, https://www.gurufocus.com/term/operatingmargin/GOOG/Operating%252BMargin/Alphabet%2BInc [https://perma.cc/M9TK-JKR8] (last visited Apr. 4, 2019).

as supracompetitive and that derive from a market that Google dominates. Since 2004, Alphabet has purchased close to 200 companies.[564] Several of these acquisitions strengthened Google's position in digital advertising, its core market.[565] But many of its purchases have established its position in new markets; indeed, Alphabet has built its strength outside of advertising almost entirely through acquisitions.[566] Google established its home-automation business,[567] for example, primarily through buy-ups.[568] Most recently, the race

564. Vicky Huang, Google Has Acquired 200 Companies Since 2001—Here Are Its Biggest Failures, Street (Jan. 14, 2017), https://www.thestreet.com/story/13952508/1/google-s-moonshots-make-crash-landing.html [https://perma.cc/7TVB-7XGD]; see also Josh Lipton, Google's Best and Worst Acquisitions, CNBC (Aug. 19, 2014), https://www.cnbc.com/2014/08/19/googles-best-and-worst-acquisitions.html [https://perma.cc/284M-ZE3M].

565. In the second quarter of 2017, 86% of Alphabet's total revenue came from advertising alone. Matthew Reynolds, If You Can't Build It, Buy It: Google's Biggest Acquisitions Mapped, Wired (Nov. 25, 2017), http://www.wired.co.uk/article/google-acquisitions-data-visualisation-infoporn-waze-youtube-android [https://perma.cc/U8ZW-LVBF]. Acquisitions that boosted its ad business include YouTube ($1.65 billion in 2006) and DoubleClick ($3.1 billion in 2007). Id.

566. For example, its 2005 purchase of Android (for an undisclosed but reported price of $50 million) launched the company into the market for wireless device operating systems. It was described as the "best deal ever" by an Alphabet executive. Owen Thomas, Google Exec: Android Was "Best Deal Ever," VentureBeat (Oct. 27, 2010), https://venturebeat.com/2010/10/27/google-exec-android-was-best-deal-ever/ [https://perma.cc/K5VM-5M62]. The Android acquisition set up Google to enter the market for mobile ads, which generated over $49 billion in annual revenue for the company in 2017. Rani Molla, Google Leads the World in Digital and Mobile Ad Revenue, Recode (July 24, 2017), https://www.recode.net/2017/7/24/16020330/google-digital-mobile-ad-revenue-world-leader-facebook-growth [https://perma.cc/9MHL-4ATB]. Today, Android captures around 88% of the global smartphone market. Ananya Bhattacharya, Android Just Hit a Record 88% Market Share of All Smartphones, Quartz (Nov. 3, 2016), https://qz.com/826672/android-goog-just-hit-a-record-88-market-share-of-all-smartphones/ [https://perma.cc/2ML2-4NCQ]. Embedding sensors in Android products, in turn, has let Alphabet collect enormous amounts of location data, which it feeds back into its advertising business and into its maps business (both Google Maps and Waze). See Keith Collins, Google Collects Android Users' Locations Even When Location Services Are Disabled, Quartz (Nov. 21, 2017), https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/ [https://perma.cc/UEW2-78AE] (noting that Google "allow[s] advertisers to target consumers using location data"); Tim Stenovec, Google Has Gotten Incredibly Good at Predicting Traffic—Here's How, Bus. Insider (Dec. 18, 2015), https://www.businessinsider.com/how-google-maps-knows-about-traffic-2015-11 [https://perma.cc/2BKF-8N93] ("Hundreds of millions of people around the world give Google real-time data that it uses to analyze traffic and road conditions."). In other words, Alphabet acquired its way into the mobile OS market, which in turn has boosted its ad and maps businesses.

567. Dan O'Shea, Google Gunning for Amazon's Smart Speaker Market, Retail Dive (Jan. 29, 2018), https://www.retaildive.com/news/google-gunning-for-amazons-smart-speaker-market/515739/ [https://perma.cc/5ANB-QL3G]. Google currently captures around 40% of the market. Id.

568. See Alistair Barr, Google's Nest Buys Smart Home Startup Revolv, Wall. St. J. (Oct. 24, 2014), https://blogs.wsj.com/digits/2014/10/24/googles-nest-buys-smart-home-startup-revolv/ (on file with the *Columbia Law Review*) (stating that Google's purchases include Nest Labs ($3.2 billion), Dropcam ($555 million), and Revolv (undisclosed)).

for capturing the AI market is spurring a new flurry of acquisitions.[569] Its pattern of acquisitions suggests that the company "will continue to push into entirely new areas, from genomics and healthcare to autonomous transport."[570]

A dominant digital platform that uses its supracompetitive profits to buy its way into other markets can raise entry barriers in two ways. First, the platform can bundle its various services, such that any new firm seeking to compete in any one line of business may be unable to enter unless it could enter in multiple lines.[571] Second, entering multiple markets positions a digital platform to combine multiple sources of data, potentially enabling a "super-platform" to control "key portals of data, which helps it attain or maintain its power across many products."[572] Amazon's growing suite of acquisitions—which have picked up since Amazon Web Services (AWS) started reporting enormous profits[573]—has also led analysts to speculate that Amazon uses AWS profits to finance entry into new markets.[574]

---

569. See Jacques Bughin et al., McKinsey Glob. Inst., Artificial Intelligence: The Next Digital Frontier? 6 (2017), https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx [https://perma.cc/J98W-KCZC] ("Companies at the digital frontier—online firms and digital natives such as Google and Baidu—are betting vast amounts of money on AI. We estimate between $20 billion and $30 billion in 2016, including significant M&A activity."). "Artificial intelligence is poised to unleash the next wave of digital disruption" and could be a $126 billion business by 2025. Id. at 4, 6.

570. Reynolds, supra note 565 (internal quotation marks omitted) (quoting Suranga Chandratillake, general partner at Balderton Capital, a London-based venture capital firm); see also Rani Molla, Google Parent Company Alphabet Has Made the Most AI Acquisitions, Recode (May 19, 2017), https://www.recode.net/2017/5/19/15657758/google-artificial-intelligence-ai-investments [https://perma.cc/CR88-ABBD].

571. See Robert D. Buzzell, Is Vertical Integration Profitable?, Harv. Bus. Rev. (Jan. 1983), https://hbr.org/1983/01/is-vertical-integration-profitable [https://perma.cc/L4RU-YYB3] ("The more vertically integrated a business, the greater the financial and managerial resources required to enter and compete in [that market]").

572. Stucke & Grunes, supra note 26, at 137.

573. While the company traditionally operated on losses or razor-thin margins, it now reports consistent profits—in large part due to AWS. See Stephanie Condon, In 2018, AWS Delivered Most of Amazon's Operating Income, ZDNet (Jan. 31, 2019), https://www.zdnet.com/article/in-2018-aws-delivered-most-of-amazons-operating-income/ [https://perma.cc/W973-6JCZ]. Called the "cash cow" of Amazon, AWS enjoys 35% of the cloud computing market, more than its next three competitors combined. Ron Miller, AWS Continues to Rule the Cloud Infrastructure Market, TechCrunch (Oct. 30, 2017), https://techcrunch.com/2017/10/30/aws-continues-to-rule-the-cloud-infrastructure-market/ [https://perma.cc/MHT2-ZJ5G].

574. Amazon has also made a suite of acquisitions to establish its position in new or early-stage lines of business. Since 1995, it has made around 130 acquisitions or investments. Zoe Henry, Amazon Has Acquired or Invested in More Companies Than You Think—At Least 128 of Them, Inc. (May 2017), https://www.inc.com/magazine/201705/zoe-henry/will-amazon-buy-you.html [https://perma.cc/9KC6-BL35]. Its largest purchases include Audible (audiobooks, $300 million), Zappos (shoes, $1.2 billion), Kiva Systems (robotics, $775 million), Annapurna Labs (semiconductor chip designer, $370 million), Twitch Interactive (video game livestreaming, $970 million), and Whole Foods (grocery, $13.7 billion). Jeff Desjardins,

The desire to prevent companies from extending their existing dominance into new lines of business motivated policymakers to impose structural limits on firms with government-granted advantages.[575] Unlike in the case of telephone carriers, the additional costs of these new ventures are not raising government-set rates that the public must pay.[576] But if durable and persistent dominance is enabling a platform to earn supracompetitive profits that it can sink into any new market it chooses to enter, the dynamic may raise analogous concerns, especially given that dominant platforms' serial acquisitions—431 over the last decade[577]—appear to have helped them maintain and extend their dominance.[578]

Placing structural limits to address this concern would require separating the business earning supracompetitive profits from other businesses. This would not necessary fall along the line of separating platforms from commerce. Although in other contexts the functional goal of preventing protected profits from financing entry into new markets aligned with the goal of preventing conflicts of interest, in this context the two goals may yield different forms of breakup.

b. *Media Diversity.* — As in the past, integration by dominant platforms today could undermine the richness and diversity of outlets providing media and news. At first blush, this may seem counterintuitive, given how much easier and cheaper the digital age has made it to disseminate information. But the proliferation of information in the digital age—the age of information overload—means that the firms organizing and delivering desired and valued information gain in importance. The dominant platforms have emerged as powerful gatekeepers and network distributors in part because they serve as digital portals, and "choosing and switching among different portals entails cognitive costs."[579] This stickiness helps explain why a portal that achieves early dominance can prove so challenging to dislodge.

Infographic: Amazon's Biggest Acquisitions, Bus. Insider (Sept. 12, 2017), http://www.businessinsider.com/amazon-stock-price-biggest-acquisitions-infographic-2017-9 [https://perma.cc/EP9N-AAD4]; Sally French, All the Companies in Jeff Bezos' Empire, in One (Large) Chart, MarketWatch (Jan. 30, 2018), https://www.marketwatch.com/story/its-not-just-amazon-and-whole-foods-heres-jeff-bezos-enormous-empire-in-one-chart-2017-06-21 [https://perma.cc/EM5T-U8JT].

575. See supra section IV.B.

576. See Shelanski, Adjusting Regulation, supra note 350, at 59–60 (describing government-set rates in the telephone industry as a response to concerns about monopolies).

577. David McLaughlin, Did Big Tech Get Too Big? More of the World Is Asking, Bloomberg (Mar. 21, 2019), https://www.bloomberg.com/news/articles/2019-03-22/did-big-tech-get-too-big-more-of-the-world-is-asking-quicktake (on file with the *Columbia Law Review*) ("Data compiled by Bloomberg show the big five—Alphabet, Amazon, Apple, Facebook and Microsoft—have made 431 acquisitions worth $155.7 billion over the last decade.").

578. See supra Part I.

579. John M. Newman, Antitrust in Digital Markets, 72 Vand. L. Rev. (forthcoming 2019) [hereinafter Newman, Digital Markets] (manuscript at 10) (on file with the *Columbia Law Review*).

Critics have argued that Amazon's outsized power to cut off publishers and authors from the online marketplace threatens First Amendment values.[580] Google and Facebook's role as dominant portals of news and media, meanwhile, may undermine the health and diversity of the media ecosystem. For one, the need to be visible in search rankings and the News Feed incentivizes publishers to invest in content that the platforms' algorithms favor. Facebook's emphasis on video content, for example, spurred publishers to fire hundreds of journalists in favor of video producers—only to learn that Facebook had inflated its video numbers.[581] A market structure in which two companies set the metrics determining whether internet content gets seen is not a system that promotes diversity. In recent years, questions about news bias by Facebook and the black-box nature of Google search rankings have prompted a larger discussion about whether permitting two firms to capture control over digital information mediation undermines the integrity of our news ecosystems.[582]

This algorithm-chasing dynamic is primarily a feature of Google and Facebook's horizontal dominance. But Facebook and Google also vertically compete with the news publishers that depend on their platforms for greater exposure to readers.[583] This dual role they play—as a competitor in the sale of digital ads and as an intermediary in the distribution of information—diverts advertising revenue from publishers to the dominant platforms, helping them maintain their duopoly in the digital advertising market.[584] The news industry, meanwhile, is on life support: Hundreds of local and regional newspapers have

---

580. See Letter from Authors United to William J. Baer, Assistant Att'y Gen., Antitrust Div., Dep't of Justice, http://www.authorsunited.net/july/longdocument.html [https://perma.cc/76GZ-38KW] (last visited Oct. 21, 2018) ("Amazon's aggressive and retaliatory behavior has engendered fear and stifled expression throughout the book industry. As we can attest from our own experience at Authors United, such fear runs deep among authors, editors, and literary agents.").

581. Alexis C. Madrigal & Robinson Meyer, How Facebook's Chaotic Push into Video Cost Hundreds of Journalists Their Jobs, Atlantic (Oct. 18, 2018), https://www.theatlantic.com/technology/archive/2018/10/facebook-driven-video-push-may-have-cost-483-journalists-their-jobs/573403/ [https://perma.cc/R68G-YT39] ("As media companies desperately tried to do what Facebook wanted, many made the disastrous decision to 'pivot to video,' laying off reporters and editors by the dozen."); see also Nicholas Thompson & Fred Vogelstein, Inside the Two Years that Shook Facebook—and the World (Feb. 12, 2018), https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/ [https://perma.cc/5E45-DTRB] ("Every publisher knows that, at best, they are sharecroppers on Facebook's massive industrial farm.").

582. See Foer, supra note 4, at 123–27 (arguing that Google, Facebook, and Amazon are "indifferent to democracy" and yet "have acquired an outside role in it"); Frank Pasquale, The Black Box Society 71 (2015) (describing how the vast array of content provided by Facebook's "News Feed" may favor the interests of advertisers and Facebook itself over the news-consuming public).

583. See supra section I.C; see also Elisa Shearer & Jeffrey Gottfried, News Use Across Social Media Platforms 2017, Pew Research Ctr. (Sept. 7, 2017), https://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/ [https://perma.cc/3NBG-VXV9] (finding that 45% of U.S. adults get news through Facebook).

584. See supra sections I.B–.C.

been rolled up or shuttered, such that two thirds of counties in America now have no daily newspaper and 1,300 communities have lost all local coverage.[585] Even outlets native to the web, like Buzzfeed and the Huffington Post, are laying off reporters.[586]

Insofar as this dual role played by Facebook and Google deprives publishers of digital advertising revenue, structurally separating the communications networks these firms operate from their ad businesses could potentially be justified on the basis of protecting the news media. Rather than separating platforms from commerce, such a separation would target a particular business model in order to promote media diversity and protect journalism.[587] Careful analysis would be needed to determine precisely what kinds of limits on behavioral-ad based business models might be justified.

c. *System Resiliency.* — As a growing share of online commerce and communications rely on dominant online platforms, the resiliency of platform infrastructure becomes paramount. Yet concentrating activity can also concentrate risk, creating the possibility that a single system crash could have cascading effects.[588]

---

585. Riley Griffin, Local News Is Dying, and It's Taking Small Town America With It, Bloomberg (Sept. 5, 2018), https://www.bloomberg.com/news/articles/2018-09-05/local-news-is-dying-and-it-s-taking-small-town-america-with-it (on file with the *Columbia Law Review*); Tom Stites, About 1,300 U.S. Communities Have Totally Lost News Coverage, UNC News Desert Study Finds, Poynter (Oct. 15, 2018), https://www.poynter.org/business-work/2018/about-1300-u-s-communities-have-totally-lost-news-coverage-unc-news-desert-study-finds/ [https://perma.cc/Z87F-E999].

586. Oliver Darcy & Tom Kludt, Media Industry Loses About 1,000 Jobs as Layoffs Hit News Organizations, CNN (Jan. 24, 2019), https://edition.cnn.com/2019/01/24/media/media-layoffs-buzzfeed-huffpost-gannett/index.html [https://perma.cc/D2MU-NVDD].

587. Responding to the rise of the new information monopolies, Professor Tim Wu has argued in favor of applying a separations regime in information industries, specifically an approach that would create "a salutary distance between each of the major functions or layers in the information economy." Tim Wu, The Master Switch 304 (2010).

588. For in-depth analysis of how excessive concentration can heighten system fragility, see generally Barry C. Lynn, End of the Line: The Rise and Coming Fall of the Global Corporation 11 (2005) (arguing that an essential network platform "can be viewed as common property that belongs to all of the companies that rely on it" and therefore, "no one, quite naturally, is responsible for ensuring that the system is safe"); Barry C. Lynn, Built To Break, Challenge, Mar.–Apr. 2012, at 87, 94–95 (describing a shutdown in Japanese automobile manufacturing following a 2007 earthquake, which disrupted operations at an industrial firm that produced an automobile part used by all Japanese automakers, and using this example to illustrate the problems that result when an entire industry utilizes the same infrastructure); Yossi Sheffi & Barry C. Lynn, Systemic Supply Chain Risk, Bridge, Fall 2014, at 22, 25–26 (noting how, given increasing reliance on "single 'super' suppliers" throughout the economy, "[a] strike, sabotage, financial problem, or cyber-attack can shut down a supplier, . . . creating a systemic disruption"). For an argument for why antitrust analysis generally and merger enforcement specifically should take fragility and resiliency concerns into account, see Peter C. Carstensen & Robert H. Lande, The Merger Incipiency Doctrine and the Importance of "Redundant" Competitors, 2019 Wis. L. Rev. (forthcoming) (manuscript at 58–63) (on file with the *Columbia Law Review*).

For example, AWS leads the cloud computing market, capturing a greater share than its next three competitors combined.[589] This level of concentration has at least two potential risks. One is general fragility. For example, a single outage at AWS a few years ago led Netflix, Reddit, Business Insider, and several other major websites to crash for five hours.[590] The second risk is the security vulnerabilities created by monoculture. Homogeneity can render a system more susceptible to malware or hacks, a risk recognized in the context of computer systems.[591] As more businesses come to use AWS as default computing power (the company counts among its clients the CIA[592]), the potential systemic ramifications are not trivial. Indeed, the prospect of Amazon winning a single-source contract for the Pentagon has prompted concerns that awarding the business to a single provider could increase cybersecurity risks.[593] Analogous concerns raised by Google's dominance have prompted policy officials to debate whether the company should be designated as "critical infrastructure."[594]

Notably, these resiliency concerns are primarily responding to concentration, not integration. A vertical separation would not address the underlying issue, unless exiting an adjacent market would reduce exposure to risk.

---

589. See Peter Cohan, 5 Ways That Amazon Keeps Its Lead in the $180B Cloud, Forbes (Aug. 1, 2018), https://www.forbes.com/sites/petercohan/2018/08/01/5-ways-that-amazon-keeps-its-lead-in-the-180b-cloud/ [https://perma.cc/V6EW-DYZD].

590. Romellaine Arsenio, Amazon Web Services Suffers Crash, Takes Down Netflix, Reddit, Tinder and Other Huge Parts of The Internet, Tech Times (Sept. 23, 2015), http://www.techtimes.com/articles/86667/20150923/amazon-web-services-suffers-crash-takes-down-netflix-reddit-tinder-and-other-huge-parts-of-the-internet.htm [https://perma.cc/6Z2R-KTP4].

591. The Computer & Communications Industry Association raised the issue of monoculture during the U.S. antitrust proceedings against Microsoft. A report published by the group in 2003 concluded, "The presence of this single, dominant operating system in the hands of nearly all end users is inherently dangerous. . . . These competition related security problems have been with us, and getting worse, for years." Dan Geer et al., Cyber*In*security: The Cost of Monopoly 3–4 (2003), https://www.flyingpenguin.com/wp-content/uploads/2016/02/cyberinsecurity.pdf [https://perma.cc/7QBS-K9YW].

592. Kevin McLaughlin, Amazon Wins $600 Million CIA Cloud Deal as IBM Withdraws Protest, CRN (Oct. 30, 2013), http://www.crn.com/news/cloud/240163382/amazon-wins-600-million-cia-cloud-deal-as-ibm-withdraws-protest.htm [https://perma.cc/NQE8-7HG3].

593. Ali Breland, Amazon's Attempt to Land Major Pentagon Job Stokes Antitrust Fears, Hill (Mar. 11, 2018), http://thehill.com/policy/technology/377649-amazons-attempt-to-land-major-pentagon-job-stokes-antitrust-fears [https://perma.cc/LMY8-DQ67] ("A single-source provider for Pentagon cloud services is obviously reckless. The Pentagon should clearly have multiple cloud providers so that if something happens to one of them there is resiliency and redundancy." (internal quotation marks omitted) (quoting Matt Stoller, fellow at the Open Markets Institute)).

594. See, e.g., Eric Engleman, Google Exception in Obama's Cyber Order Questioned as Unwise Gap, Bloomberg (Mar. 5, 2013), http://www.bloomberg.com/news/articles/2013-03-05/google-exception-in-obama-s-cyber-order-questioned-as-unwise-gap (on file with the *Columbia Law Review*) (describing how an executive order issued by President Obama may have exempted Google's Gmail service from being designated as "critical infrastructure").

B. *Institutional Shortcomings*

Over the last decade, antitrust agencies have primarily responded to anticompetitive vertical acquisitions through behavioral remedies.[595] Behavioral remedies include, for example, transparency provisions, information firewalls, and nondiscrimination provisions, as well as limits on certain contracting practices.[596] Unlike structural remedies, behavioral remedies seek to change the firm's conduct, while leaving the underlying incentives untouched.[597] In effect these remedies constitute "attempts to require" a merged firm to "operate in a manner inconsistent with its own profit-maximizing incentives"—an effort that proves both "paradoxical" and "likely difficult to achieve."[598]

Behavioral remedies carry at least four substantial costs.[599] First, there are the direct costs of monitoring the merged firm's activity to ensure compliance with the decree. Second, there are costs of evasion associated with the merged firm sidestepping the spirit of the decree.[600] Third, there are costs of restraining potentially procompetitive behavior.[601] And fourth, a behavioral remedy may hamper the firm's ability to adapt effectively to changing market conditions.[602] Stating that "a structural remedy can in principle avoid" these costs, the Justice Department has historically "strongly preferred" structural merger remedies to behavioral ones.[603]

The challenges of enforcing a behavioral remedy are likely heightened in digital markets, where the information asymmetry between the integrated firm and public enforcers is even starker. This is especially true with regard to information firewalls, which—in theory—could help prevent information appropriation by dominant integrated firms.[604] In practice, seeking to regulate the dissemination of information within a firm is difficult in any market—let alone in multibillion dollar markets built around the intricate collection,

595. Bureaus of Competition and Econ., FTC, The FTC's Merger Remedies 2006-2012, at 13 (2017), https://www.ftc.gov/system/files/documents/reports/ftcs-merger-remedies-2006-2012-report-bureaus-competition-economics/p143100_ftc_merger_remedies_2006-2012.pdf [https://perma.cc/CA6B-WFHN] (capturing that 100% of vertical mergers in which the Commission ordered a remedy, the remedy was non-structural).

596. Kwoka & Moss, supra note 27, at 982–83.

597. Id. at 982.

598. Id.

599. U.S. Dep't of Justice, Antitrust Division Policy Guide to Merger Remedies 8–9 (2004), https://www.justice.gov/sites/default/files/atr/legacy/2011/06/16/205108.pdf [https://perma.cc/YC9N-KYRY].

600. For example, if a remedy required a firm not to raise prices, it could go on to reduce its costs by cutting quality—"thereby effecting an anticompetitive increase in the 'quality adjusted' price." Id. at 8.

601. Id.

602. Id. at 8–9.

603. Id.

604. See supra sections I.A–.C.

combination, and sale of data.[605] The significant business insights, market intelligence, and competitive advantage derived from gathering and analyzing data suggest that firms will have an even greater incentive to combine different sets of information—meaning that any regulatory attempts to limit that sharing or dissemination is more likely to fail. The fact that these regulatory remedies are imposed by antitrust enforcers, who generally lack regulatory tools and resources,[606] makes successful oversight and compliance even more doubtful.

The Justice Department's remedies in the Google–ITA merger illustrate one instance of imposing an information firewall in a digital market. ITA developed and licensed a software product known as "QPX," a "mini-search engine" that airlines and online travel agents used to provide users with customized flight search functionality.[607] Because the merger would put Google in the position of supplying QPX to its rival travel-search websites, the Justice Department required as a condition of the merger that Google establish internal firewalls to avoid misappropriation of rivals' information.[608] Although one commentator highlighted the risks and inherent difficulties associated with designing a comprehensive behavioral remedy, the court approved the order.[609]

Whether the information firewall was successful in preventing Google from accessing rivals' business information is not publicly known. A year after the remedy expired, Google shut down its QPX API.[610]

The challenges of enforcing behavioral remedies—both generally and in digital markets specifically—highlight the importance of assessing the relative enforcement costs of alternate remedies. A focus on enforcement costs—which include administrative costs, monitoring costs, and the misallocation of

---

605. See The World's Most Valuable Resource Is No Longer Oil, but Data, Economist (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (on file with the *Columbia Law Review*) ("This abundance of data changes the nature of competition. . . . By collecting more data, a firm has more scope to improve its products, which attracts more users, generating even more data, and so on."); see also Dan Gallagher, Data Really Is the New Oil, Wall St. J. (Mar. 9, 2019), https://www.wsj.com/articles/data-really-is-the-new-oil-11552136401 (on file with the *Columbia Law Review*) ("Moving ones and zeroes around the Internet is getting to be more expensive than keeping the oil flowing.").

606. See, e.g., Delrahim, supra note 27 ("[A]ntitrust is law enforcement, it's not regulation.").

607. Competitive Impact Statement at 1–2, United States v. Google Inc., No. 1:11-CV-00688 (D.D.C. Oct. 5, 2011).

608. Id. at 13–14. The Justice Department included as a condition of the merger that Google not restrict, through exclusive dealing, its rivals' access to the airlines' seat and booking-class data. Final Judgment at 27–28, *Google Inc.*, No. 1:11-CV-00688.

609. See Eric K. Clemons & Nehal Madhani, The Real and Inevitable Harm from Vertical Integration of Search Engine Providers into Sales and Distribution, Huffington Post: The Blog (Apr. 20, 2011), https://www.huffpost.com/entry/the-department-of-justice_b_851079 [https://perma.cc/9KC2-6E5A].

610. Ingrid Lunden, Google Will Pull Its QPX Express API in April 2018, Cutting Off Its Airfare Feed, TechCrunch (Nov. 1, 2017), https://techcrunch.com/2017/11/01/google-will-pull-its-qpx-express-api-in-april-2018-cutting-off-its-flight-data-feed/ [https://perma.cc/CRA5-PEZ3].

resources resulting from rent-seeking activity[611]—can help identify instances when the purported welfare benefits of a conduct remedy may not be worth the steep enforcement costs. Another factor to consider is the prospect that rejecting a structural remedy earlier could result in more regulation later. This prospect is especially likely in monopolistic markets, where the failure to build an "effective institutional firewall between the regulated monopoly and the other segments of a vertical chain" could mean that "as the number of competitive interfaces between regulated monopoly and competitive segments expands, the regulation of these competitive interfaces will expand as well."[612] In other words, cabining the monopoly can cabin regulation.

Lastly, it is worth considering whether increases in information asymmetries between companies and enforcers should weigh in favor of greater reliance on structural remedies. If enforcers have less ability to discern a firm's business activities—be it due to heightened opacity or complexity—then targeting the firm's incentives, rather than attempting to police its behavior, may make more sense.

C. *Theory*

One condition that generally united previous separations is that they were applied to bottleneck firms. This was true in both the regulated industries and antitrust contexts.[613] The regulated-industries paradigm identified dominant intermediaries through functional criteria rather than strict economic ones. Although most regulated industries exhibited natural monopoly features, separations were often implemented not—as natural monopoly regulation is sometimes described—to correct market failure but instead to promote goals that privately regulated markets could not deliver.[614] Antitrust separations, meanwhile, sought to remedy abuses of monopoly power.[615] In either case, separations were responding to the dominance of a gatekeeper entity.[616] In regulated industries, outsized market power was what rendered a firm's

611. Shelanski & Sidak, supra note 18, at 19.

612. Joskow & Noll, supra note 462, at 1253.

613. See supra Part III.

614. As Professors Kearney and Merrill note, the application of regulated industries law was guided less by the designation of national monopoly industries and more by a belief that "government oversight of the market was required to ensure the accepted goals of reasonableness, non-discrimination, and reliable service." Kearney & Merrill, supra note 232, at 1334; see also Nachbar, supra note 240, at 102 ("[T]he correlation between market power and the traditional imposition of nondiscriminatory access is tenuous at best.").

615. When analyzing the effects of exclusionary conduct by a dominant firm, case law assesses whether rivals have access to alternative channels to market. Compare, e.g., United States v. Microsoft Corp., 253 F.3d 34, 70–71 (D.C. Cir. 2001) (en banc) (per curiam) (holding that the dominant firm's exclusionary conduct violated the antitrust laws because its rivals lacked alternative distribution channels), and United States v. Dentsply Int'l Inc., 399 F.3d 181, 196 (3d Cir. 2005) (same), with Omega Envtl., Inc. v. Gilbarco, Inc., 127 F.3d 1157, 1163 (9th Cir. 1997) (finding that the exclusive conduct at issue did not violate the antitrust laws, in part because rivals had other efficient routes to market).

616. See supra Part III.

business decisions systemically significant, while in antitrust, a lack of competition meant a lack of market discipline.

Assessing whether integration by dominant platforms might invite structural separations requires evaluating (1) whether a digital platform is dominant and serving as a gatekeeper intermediary, and (2) whether that dominance is likely to be durable and persistent, in light of high entry barriers. In other words, is it likely that, absent separations, discrimination or appropriation by these firms will be disciplined by competition? Critically, it is not discrimination or information appropriation per se that is harmful—but rather discrimination or information appropriation by a network intermediary for which there are no substitute channels to market.[617] Insofar as a platform grants access to third-party products, "a bottleneck to everything can potentially take a share of, and exercise some control over, everything."[618]

For many years, an underlying assumption regarding digital markets has been that they are characterized by "uniquely low" entry barriers.[619] Unlike

617. Given these factors, it is unlikely that a grocer selling private labels would give rise to similar harms. There is also reason to think that discrimination and appropriation in digital markets, by virtue of being more tailored and sophisticated, have a greater effect on competition than discrimination and appropriation in nondigital markets.

618. Howard A. Shelanski, Information, Innovation, and Competition Policy for the Internet, 161 U. Pa. L. Rev. 1663, 1676 (2013); see also Posner, New Economy, supra note 349, at 934 ("We may be in a similar stage in the development of the new economy, where distribution facilities may be sufficiently limited to create bottlenecks that monopolists can exploit to perpetuate monopoly.").

619. Newman, Digital Markets, supra note 579, at 14 & nn.86–88 (emphasis added) (collecting sources); see also, e.g., Am. Library Ass'n v. United States, 201 F. Supp. 2d 401, 416 (E.D. Pa. 2002), rev'd, 539 U.S. 194 (2003) ("The Internet presents low entry barriers to anyone who wishes to provide or distribute information."); Shea ex rel. Am. Reporter v. Reno, 930 F. Supp. 916, 929 (S.D.N.Y. 1996) ("[T]he Internet presents extremely low entry barriers to those who wish to convey Internet content or gain access to it."); ACLU v. Reno, 929 F. Supp. 824, 877 (E.D. Pa. 1996) ("[T]he Internet presents very low barriers to entry."); Geoffrey A. Manne & Joshua D. Wright, Google and the Limits of Antitrust: The Case Against the Case Against Google, 34 Harv. J.L. & Pub. Pol'y 171, 195 (2011) (summarizing Google's assertion "that competition really is 'just a click away' for a significant number of users" in the online search market); Henry H. Perritt, Jr., Cyberspace and State Sovereignty, 3 J. Int'l Legal Stud. 155, 161 (1997) ("[T]he most important differentiating characteristic of the Internet is its extremely low barriers to entry."); Posner, New Economy, supra note 349, at 930 ("Because of the extraordinary pace of innovation, . . . the extraordinary amount of capital that is available . . . , and the rapidity with which new networks that are primarily electronic can be put into service, the networks that have emerged in the new economy do not seem particularly secure against competition."); D. Daniel Sokol & Roisin Comerford, Antitrust and Regulating Big Data, 23 Geo. Mason L. Rev. 1129, 1136 (2016) ("Data driven markets are typically characterized by low entry barriers. . . ."); Deborah T. Tate, Net Neutrality 10 Years Later: A Still Unconvinced Commissioner, 66 Fed. Comm. L.J. 509, 518 (2014) ("The Internet's low entry costs and lack of barriers to create, upload, start up, and sell goods and services are especially beneficial to women and minorities with less access to capital than established firms."); Yana Welinder, A Face Tells More Than a Thousand Posts: Developing Face Recognition Privacy in Social Networks, 26 Harv. J.L. & Tech. 165, 189 (2012) ("[T]he Internet offers a platform for projects that require very little capital investment — thus lowering the barriers to entry."); Ilene Knable Gotts & Joseph G. Krauss, Antitrust Review of New Economy Acquisitions, Antitrust, Fall 2000, at 59, 59 (arguing that few "'new economy' transactions" raised antitrust issues because of "the low entry barriers in the Internet space").

industries involved in the production and distribution of physical goods, digital markets have been understood to involve relatively low capital investment and rapid rates of innovation.[620] Market power enjoyed by digital firms is assumed to be fleeting, constantly susceptible to the dizzying pace of technological change.[621] This general view of digital markets—as exceptionally dynamic and self-correcting—has produced a highly permissive approach to regulation and antitrust enforcement in these markets.[622]

More recently, however, new research and experience has demonstrated that digital markets can favor long-term dominance. This is due to several features. One is network effects, whereby the value of the network increases with greater use of that network.[623] Bigger is generally better. But the same demand-side economies of scale that help a network form can also come to shield the network from competition, as a potential competitor must induce a significant number of users to choose its network over the existing good or service.[624] In the absence of interconnection, the switching costs for users can be significant, making it difficult for even a rival with a superior product or service to induce users to switch.[625] Not all network effects are the same, and not all network effects serve as entry barriers. Indeed, the significance of the entry barriers created by network effects will vary depending on the strength and type of the network and on the availability of interconnection, interoperability, multihoming, and other tools that could soften these exclusionary effects.[626]

---

620. Posner, New Economy, supra note 349, at 926.

621. See Newman, Digital Markets, supra note 579, at 19–21 ("[A]nti-enforcement scholars and stakeholders contend that digital markets should evade antitrust scrutiny because 'competition is just a click away.'").

622. As Professor John Newman writes, the last two decades have been characterized by a "near-total lack of antitrust enforcement in digital markets." Id. at 4. Notably, enforcers and scholars have acknowledged that technology markets *can* be susceptible to entry barriers and anticompetitive conduct. See id. at 24–37 (describing various types of "cognizable welfare harm" that are "uniquely facilitated by digital markets"). But the assumption that false positives are highly costly, while false negatives are rare, has tilted the balance in favor of underenforcement. See id. at 56; see also Frank H. Easterbrook, The Limits of Antitrust, 63 Tex. L. Rev. 1, 2–4 (1984) ("If the court errs by condemning a beneficial practice, the benefits may be lost for good. . . . If the court errs by permitting a deleterious practice, though, the welfare loss decreases over time. Monopoly is self-destructive. Monopoly prices eventually attract entry."). It is also worth noting that dominant tech firms have benefited not only from a laissez faire approach to actions that would limit their power or autonomy, but also from other favorable government policies, including generous intellectual property rights and historically low interest rates.

623. Katz & Shapiro, supra note 284, at 483.

624. See Mark A. Lemley & David McGowan, Legal Implications of Network Economic Effects, 86 Calif. L. Rev. 479, 483 (1998) ("In other words, a network effect exists where purchasers find a good more valuable as additional purchasers buy the same good.").

625. See Frank Pasquale, When Antitrust Becomes Pro-Trust: The Digital Deformation of U.S. Competition Policy, Antitrust Chron., May 2017, at 46, 48–49 (arguing that assuming that the costs of switching between online platforms are low "belies the complexity of online innovation").

626. Lemley & McGowan, supra note 624, at 483–84.

A second feature that can favor platform dominance is heightened returns to scale. The cost structure of many digital markets involves steep up-front costs followed by low marginal costs.[627] Firms in the business of providing information see their marginal cost plummet, as information—once produced—can be disseminated online to large groups at negligible costs.[628] Increasing returns to scale can also discourage entry, as only a firm with either a far superior or far cheaper product would enter the market.[629]

A third factor that can benefit dominant incumbents is the critical and competitive significance of data.[630] Services like Google Maps, for example, have been built through collecting billions of user data inputs, operating camera-fitted cars that collected more than 21.5 billion megabytes of street-view images from around the world, and combining multiple sources of place data across various Android devices.[631] Theoretically a new firm could attempt to build a rival service by relying on public data, but the continued data inputs that Google Maps receives after achieving initial success are likely to keep any potential competitor a distant second.[632] These self-reinforcing advantages of data can amplify network effects, lead markets to tip, and close off entry.

Assessing whether a dominant platform should be subject to separations would require analyzing these factors and the degree to which they serve as high entry barriers or render merchants or trading partners "unavoidable."[633] Limiting digital dominant platforms whose services constitute a "unique infrastructural asset" from entering adjacent markets and competing with dependent trading partners could avoid distortions of the competitive process and generate a host of other payoffs.[634]

D. *Application: Challenges and Unresolved Questions*

Implementing a separations regime presents some first-order questions and challenges. First, how do we define platforms and to which platforms should a separation apply? Second, how does one identify the parameters of the platform, especially when integration provides heightened functionality? Third, what should be the scope of the prohibited activity and how should the prohibition be structured? And fourth, what is the proper institutional

---

627. Crémer et al., supra note 3, at 20.

628. Id.

629. Id.

630. See supra note 286 and accompanying text.

631. Newman, Digital Markets, supra note 579, at 15.

632. See, e.g., The Manifest, Apple Maps vs. Google Maps: Which Is Better?, Medium (Sept. 12, 2018), https://medium.com/@the_manifest/apple-maps-vs-google-maps-which-is-better-9ceaf28f9bf0 [https://perma.cc/H28R-WHCV] (noting that Google Maps remains preferred to Apple Maps by a "clear majority of smartphone owners," even though Apple has made significant improvements to its Maps application).

633. See Case T 286/09, Intel Corp. v. Commission, ECLI:EU:T:2014:547 para. 91 (E.C.J. June 12, 2014) (discussing "unavoidable trading partner").

634. For one theory of what constitutes "infrastructure," see Frischmann & Waller, supra note 295, at 11–12.

mechanism for implementing the separation? This section offers some initial suggestions for how to approach these questions. Arriving at a complete analytical framework for structuring separations in digital markets will require deeper engagement with these issues.

1. *Defining Platform.* — Offering a clearly bounded definition of "platform" is challenging. Most definitions look to the role that the entity plays in intermediating activity by others. One definition, for example, is "a firm that controls a network, facility, or essential input that those providing a complementary good or service" must "rely on."[635] Another set of definitions focuses on the infrastructure-like role that these firms play, by structuring access to markets or facilitating transactions.[636] And some discussions use the terms "network," "infrastructure," and "platform" interchangeably.[637]

Recent studies by policymakers have also settled on the idea that dominant platforms play a unique role that regulators should recognize. In March, the Digital Competition Expert Panel—a panel convened by the U.K. government to study digital markets—issued a report proposing, among other ideas, that dominant platforms that enjoy a "powerful negotiating position" be designated as having a "strategic market status" and be required to abide by a special code of conduct.[638] A report commissioned by the European Commission, meanwhile, noted that, by designing marketplace rules that govern millions of users, dominant platforms "function as regulators" that should face a special responsibility to "ensure a level playing field" on their marketplace and "not use [their] rule-setting power to determine the outcome of competition."[639]

Given the challenge of offering a bounded definition of "dominant platform," any definition will likely be under- or over-inclusive. But any definition should seek to capture the degree of market power that the platform enjoys over users.[640] How essential is the platform's infrastructure? To what degree do other businesses depend on the platform to reach users, and what is

635. Weiser, supra note 17, at 271.

636. See Khan, Antitrust Paradox, supra note 255, at 795 ("Amazon itself effectively controls the infrastructure of the internet economy."); Rahman, New Utilities, supra note 26, at 1641 ("Firms like [too-big-to-fail] finance, Verizon, Google, or Amazon provide essential public goods, not in the economistic sense of being non-rival and non-excludable, but in a broader social sense of comprising the basic *infrastructure* of modern society.").

637. As Professor Julie Cohen has noted, platforms are slightly different from infrastructures and networks; they take advantage of network effects and provide infrastructures but also "represent strategies for bounding networks and privatizing and controlling infrastructures." Julie E. Cohen, Law for the Platform Economy, 51 U.C. Davis. L. Rev. 133, 144 (2017); see also Frischmann, supra note 226, at 319–23 (describing a five-layer model of internet infrastructure).

638. Digital Competition Expert Panel, supra note 31, at 59–61.

639. Crémer et al., supra note 3, at 6.

640. It's worth noting that "platforms" can be further distinguished by type. Nick Srnicek, for example, identifies five distinct types of platforms: advertising platforms (Google, Facebook); cloud platforms (AWS, Salesforce); industrial platforms (General Electric, Siemens); product platforms (Spotify); and lean platforms (Uber, Airbnb). Nick Srnicek, Platform Capitalism 49 (2016).

the cost to businesses of avoiding this platform and using alternative channels? Relevant factors could include: (1) the extent to which the entity serves as a central exchange or marketplace for the transaction of goods and services, including the level of market power that it enjoys in its platform market; (2) the extent to which the entity is essential for downstream productive uses, and whether downstream users have access to viable substitutes for the entity's services; (3) the extent to which the entity derives value from network effects, and the type of network effects at play; (4) the extent to which the entity serves as infrastructure for customizable applications by independent parties; and (5) the size, scope, scale, and interconnection of the company.

There are no neatly bounded ways to capture these dimensions of platform power. When implementing "maximum separation," the FCC initially used operating revenue as the criterion for determining which carriers must comply.[641] In the context of digital platforms, market share may prove a better proxy than operating revenues, given that it is the platform's role as a gatekeeper or bottleneck—for which there are no real adequate substitutes—that gives rise to the relevant harms.

The prohibition should be centered on the activities that the platform facilitates as a bottleneck. Since a key goal of the separations regime is to eliminate the conflict of interest that arises when a dominant platform directly competes with the firms using the platform,[642] only activity that would place platforms in direct competition in this way would be subject to the prohibition. This would not prevent platforms from integrating into lines of business that do not rely on the platform market. Nor would such a separations regime target conglomeration or vertical integration categorically; it would instead focus on platform entry into markets that creates the ability and incentive to discriminate, to leverage dominance, and to use information collected on firms as customers against them as competitors.

2. *Distinguishing Between Platform and Commerce.* — Applying separations to digital platforms would likely raise the challenge of identifying what constitute distinct products or services. In *Microsoft*, for example, the court had to determine whether the operating system and the browser—the two products the government claimed Microsoft had "tied"—should be considered a single integrated system.[643] Microsoft argued that bundling new functionality

---

641. See *Computer I*, 28 F.C.C.2d 291, 302–03, para. 36 (1970) (tentative decision). The FCC determined that maximum separations applied only to carriers whose combined annual operating revenue exceeded $1 million. Id. Its policy justification was to avoid imposing burdens on smaller carriers, which it thought could spur competition in data processing. See id. at 299, para. 25. It acknowledged arguments that small carriers could also discriminate or abuse powers if permitted to enter data processing but concluded that "both the potential and motives for abuse by these smaller carriers is minimal at this time." *Computer I*, 28 F.C.C.2d 267, 275, para. 23 (1971) (final decision and order).

642. See section IV.A.

643. See United States v. Microsoft Corp., 253 F.3d 34, 84–89 (D.C. Cir. 2001) (en banc) (per curiam) ("[U]nless products are separate, one cannot be 'tied' to the other.").

into old products was a basic component of technological evolution.[644] A similar issue may arise with digital platforms: Android, for example, could claim that certain apps must be integrated with its operating system in order to provide basic functionality or for technical necessity.

The traditional metric for assessing whether a set of bundled products constitute separate products is consumer demand. In *Microsoft*, the D.C. Circuit relied on *Jefferson Parish*'s consumer-demand test to determine whether consumers preferred a choice in browsers.[645] Applying a similar inquiry in the platform context could similarly help identify whether integration of distinct functionalities should be viewed as an integrated system or as a platform.

Regulators would also have the capacity to determine, over time, whether certain apps or features were necessary for basic functionality and whether the benefits of integration were sufficiently high to offset any potential harms to innovation. There may also be specific apps or functionalities where innovation is less likely to be transformative, and therefore where integration may prove fewer risks. As with earlier regimes, periodic reassessment and revisions would prove necessary to ensure the separation continued to accord with and reflect evolving market realities.

3. *Institutional Mechanism and Timing.* — A separations regime separating platforms and commerce could be implemented through statute or rulemaking or as antitrust remedies (under existing or new antitrust law). A statute from Congress could also establish the principle of separating platforms from commerce—as was the case with banking—with the specific authority to design and implement separations delegated to an agency. This approach would benefit from having an expert agency design and revisit the separation. Absent new legislation, the FTC could use its Section 5 authority to implement a separations principle through rulemaking.[646] Designing separations only

644. See id. at 85 ("Microsoft does not dispute that it bound Windows and IE in the four ways the District Court cited. Instead it argues that Windows (the tying good) and IE browsers (the tied good) are not 'separate products' . . . .").

645. Id. at 89; see Jefferson Parish Hosp. Dist. No. 2 v. Hyde, 466 U.S. 2, 12 (1984) ("[T]he essential characteristic of an invalid tying arrangement lies in the seller's exploitation of its control over the tying product to force the buyer into the purchase of a tied product that the buyer either did not want . . . or might have preferred to purchase elsewhere on different terms.").

646. In *National Petroleum Refiners Ass'n v. Federal Trade Commission*, the D.C. Circuit held that the FTC has substantive rulemaking power under Section 5 for both "unfair methods of competition" and "unfair or deceptive acts and practices." 482 F.2d 672, 674–78 (D.C. Cir. 1973). Shortly after the decision, Congress passed the Magnuson-Moss Warranty Act, raising the procedural hurdles the FTC must jump when engaging in "unfair or deceptive acts and practices" rulemaking. Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637, sec. 202(a), § 18, 88 Stat. 2183, 2193–98 (1975) (codified as amended at 15 U.S.C. § 57a (2012)). While these hurdles cause significant delay, they do not affect the FTC's rulemaking under "unfair methods of competition," which is what the Commission could use to implement a separations regime. For more on the FTC's rulemaking authority, see Jeffrey S. Lubbers, It's Time to Remove the "Mossified" Procedures for FTC Rulemaking, 83 Geo. Wash. L. Rev 1979, 1985–87 (2015) (describing past FTC rulemakings under various statutory regimes); Sandeep Vaheesan, Resurrecting "A Comprehensive Charter of Economic Liberty": The Latent

through rulemaking would require the agency to create rules of general applicability and—absent a specific congressional mandate—could limit the agency's ability to structure highly tailored separations. Antitrust remedies would be costlier and take significantly longer, requiring the government or a private party to successfully show anticompetitive conduct and effects stemming from a digital platform's involvement in multiple markets. Given the enfeebling of antitrust doctrines that police single-firm anticompetitive conduct—and the judicial requirement that remedies be carefully tailored to competitive harm—this path is likely to be significantly more challenging.[647]

Previous instances of structural separations offer a few models for structuring these prohibitions. An operational or functional separation requires the firm to create separate divisions within the firm, requiring that a platform wishing to engage in commerce may do so only through a separate and independent affiliate, which the platform may not favor in any manner. A full structural separation, by contrast, requires that the platform activity and commercial activity be undertaken through separate corporations with distinct ownership and management. For example, the functional approach would permit Alphabet to operate Google search and vertical services that produce content so long as the two complementary services are structured as separate affiliates. The second option would prohibit Alphabet from running both the platform service and the complementary service, requiring that one be spun off and run by an independent owner.

It's not clear that anything short of a full structural separation would be sufficient, especially given the risks of information misappropriation. While running complementary services as affiliates could be accompanied by information firewalls, the efficacy of firewalls requires close monitoring.[648] Evidence shows that the antitrust agencies have neglected to fully monitor and enforce conduct remedies in the past.[649] Moreover, firewalls may prove especially difficult to monitor in the context of digital platforms, given the heightened information asymmetries between private platform firms and public enforcers. It is possible that the risk of information misappropriation may vary by platform—but dominant platforms should carry the burden of establishing why operating complementary services as affiliates would not be anticompetitive.

Power of the Federal Trade Commission, 19 U. Pa. J. Bus. L. 645, 651–57 (2017) (giving the statutory and jurisprudential bases for the FTC's authority to interpret Section 5).

647. Supra section II.B.

648. The Justice Department acknowledges this: "Effective monitoring also is required to ensure that the firewall provision is adhered to and is effective." U.S. Dep't of Justice, Antitrust Division Policy Guide to Merger Remedies 14 (2011), https://www.justice.gov/sites/default/files/atr/legacy/2011/06/17/272350.pdf [https://perma.cc/7XRE-4XFF].

649. Kwoka & Moss, supra note 27, at 989–96. Indeed, Assistant Attorney General for the Antitrust Division Makan Delrahim recently admitted that the antitrust agencies "have struggled more and more with the challenges of crafting and enforcing effective behavioral relief" and find it "difficult to monitor and enforce granular commitments like non-discrimination and information firewalls." Delrahim, supra note 27.

Finally, a basic challenge facing regulators and enforcers when dealing with high-tech industries is the role of timing. Because these markets can evolve quickly, market changes can render regulatory interventions obsolete.[650] Similarly, the failure to intervene can leave exclusionary conduct unchecked, resulting in path-dependent reductions in innovation. Any subsequent attempt to impose separations should include a built-in review process every two to three years, to ensure that the remedy still matches the market conditions.[651]

E. *Costs and Tradeoffs*

Separations may come at a cost. Vertical relations can generate certain efficiencies that structural limits forego. This section reviews some of the potential costs and tradeoffs of a separations regime, and it considers how separations might be structured to minimize potential harms and maximize countervailing benefits.

First, insofar as integration can eliminate double markups, it is possible that limiting a network monopolist's ability to compete on its own network would sacrifice certain cost savings, resulting in higher prices.[652] This loss in static efficiency should be weighed against the innovation benefits that would likely result from creating an ecosystem in which the platform lacks the incentive and ability to exclude or appropriate from third-party complementors.[653]

Second, separations could come at the expense of *platform* innovation. Prohibiting dominant platforms from competing in markets that the platform operates would reduce platform investment in certain platform-adjacent markets.[654] Insofar as directly competing with complementors can generate for a dominant platform additional profits, uniquely valuable business intelligence, and greater leverage over complementors, closing off this avenue of business

650. Judge Posner described this tension as "the tension between law time and new-economy real time." Posner, New Economy, supra note 349, at 939.

651. As scholars have observed, agencies already engage in this sort of periodic reassessment. See Wendy Wagner et al., Dynamic Rulemaking, 92 N.Y.U. L. Rev. 183, 184–90 (2017) ("In contrast to the prevailing view that agencies rarely revise rules, our findings reveal that, at least in some quarters of the administrative state, revisions are the rule rather than the exception.").

652. See supra notes 269–271 and accompanying text (describing the Chicago School theory of vertical integration and double marginalization).

653. See Caves & Singer, supra note 292, at 2, 6–11 (describing how platforms' participation in the market can decrease "edge innovation"—"the reduction in investment, entrepreneurial, and risk-taking activity by independent [app] and content providers operating at the 'edge' of a dominant platform"); Zhu, supra note 204, at 24–26 (summarizing empirical studies showing that "[the platform's] entry pushes . . . app developers to innovate in other product spaces, which may reduce wasted efforts in developing . . . duplicate apps," but in the long term, "existing or prospective complementors discouraged by [the platform's] entry may bring fewer innovative products to the platform").

654. See Caves & Singer, supra note 292, at 7.

could reduce platform profits, diminishing the platform's incentive to invest.[655] Again, this potential reduction in platform innovation would need to be weighed against the likely increase in complementor innovation—as well as the potential for greater competition in the platform market.[656] It is possible that separations could spur development of competing platforms, allowing smaller intermediaries to continue developing into viable alternatives to incumbents.

Whether we should privilege platform or complementor innovation is, in turn, a question of whether decentralized or centralized innovation should be favored.[657] The answer is likely to vary by industry and market.[658] But innovation literature suggests that "external" innovation is more valuable for two reasons.[659] First, "external innovation is more likely to be of a disruptive nature,"[660] that which marks a "radical departure from the past."[661] And second, even "disruptive" internal innovation can be contingent on the existence of external competitors.[662] For this reason, it may make sense to structure an ecosystem that encourages external innovation, even if it comes at the expense of some platform innovation.

Third, some argue that separations would dampen entrepreneurial investment by creating a barrier to exit.[663] Since venture capitalists invest in startups in order to reap the rewards of "scaling a venture to exit," this argument holds, closing off one exit path would deter investment and chill business formation.[664] It is worth noting that a policy preventing dominant platforms from competing in the very markets they mediate would leave the vast majority of exit options totally unaffected. The policy would not categorically limit vertical acquisitions or acquisitions more generally by a dominant platform. Limits would apply only if a dominant platform that

---

655. Id. ("[W]ith more enforcement, *platform* innovation could decrease due to the reduced incentive for existing or would-be platforms to invest; for example, a regime that shared the majority of the rents of incumbent platforms with edge providers or rival platforms could upset Schumpeterian competition.").

656. Id. at 6–11.

657. Van Schewick, Internet Architecture, supra note 217, at 298 ("Does decentralized innovation by many innovators offer specific advantages that cannot be achieved by a potential increase in centralized application-level innovation by a few network providers?").

658. See Lemley, supra note 210, at 651–52 (arguing that the "relationship between market structure and innovation is industry-specific," demanding a more industry-specific innovation policy).

659. Wu, Taking Innovation Seriously, supra note 213, at 318.

660. Id.

661. Lemley & Lessig, supra note 16, at 962.

662. See Wu, Taking Innovation Seriously, supra note 213, at 318 ("That is to say, established firms tend to innovate when they actually face a challenge from a startup or an outsider.").

663. See D. Daniel Sokol, Vertical Mergers and Entrepreneurial Exit, 70 Fla. L. Rev. 1357, 1362 (2018). It's worth noting that Sokol is counsel at Wilson Sonsini, which counts Google among its clients.

664. See id. ("Vertical merger policy that would unduly restrict large tech firms from undertaking acquisitions in industries as diverse as finance, pharmaceuticals, medical devices, hardware, and internet platforms would hurt incentives for innovation in the economy by chilling business formation in start-ups.").

controlled a key distribution channel or marketplace sought to acquire a firm that would compete in that marketplace. It seems unlikely that such a targeted and limited restriction—that would affect each dominant platform differently, given the distinct markets in which each is dominant—would meaningfully undermine investment. Moreover, in an environment in which startups face a threat of appropriation and discrimination by the platforms on which they are reliant, dramatically reducing the likelihood of that threat should spur some investment, not categorically diminish it.[665] Even if closing off a small number of exit options altered some investment decisions, the impact on innovation is likely to be ambiguous at worst. This is especially likely to be true in light of research showing that incumbent firms may acquire innovative startups in order to squash their research and thwart future competition[666] and that "some limited antitrust restrictions on startup acquisitions by highly-dominant incumbents would be socially beneficial."[667] Introducing this limit as a presumption would increase administrability, leading to significant administrative savings.

Applying a separations regime, however structured, will involve unavoidable uncertainties. But this uncertainty is not a compelling argument for inaction. The fact that enforcers did not block a single one of the over 400 acquisitions made by the five largest dominant platforms over the last ten years strongly suggests systemic underenforcement.[668] Switching the presumption under a limited set of conditions—namely, when a dominant platform seeks to acquire a firm that would give the platform the incentive and ability to discriminate and appropriate against third-party platform dependents—is likely to involve some costs and significant benefits.[669]

F. *Alternative Remedies*

It is worth briefly assessing what alternate remedies might address information appropriation and discrimination by dominant digital platforms.

---

665. See Caves & Singer, supra note 292, at 7–11 (describing the disincentive to invest in startups that create products platforms might copy).

666. Colleen Cunningham, Florian Ederer & Song Ma, Killer Acquisitions 1 (Mar. 22, 2019) (unpublished manuscript), http://ssrn.com/abstract=3241707 (on file with the *Columbia Law Review*) (leveraging theoretical and empirical evidence to argue that "an incumbent firm may acquire an innovative target and terminate development of the target's innovations to preempt future competition").

667. Kevin A. Bryan & Erik Hovenkamp, Antitrust Limits on Startup Acquisitions, Rev. Indus. Org. (forthcoming 2019) (manuscript at 20–21), http://ssrn.com/abstract=3350064 (on file with the *Columbia Law Review*) (suggesting that enforcers should intervene when "(a) the acquirer is highly dominant; and (b) the acquired technology could plausibly have an appreciable impact on competition if it is used exclusively by the acquirer").

668. See Digital Competition Expert Panel, supra note 31, at 12 (noting that "[o]ver the last 10 years the 5 largest firms have made over 400 acquisitions globally" but that "[n]one has been blocked and very few have had conditions attached to approval, in the UK or elsewhere," and recommending "more frequent and firmer action to challenge mergers").

669. See generally Robert W. Crandall, The Failure of Structural Remedies, 80 Or. L. Rev. 109 (2001); Richard A. Epstein, Monopolization Follies: The Dangers of Structural Remedies Under Section 2 of the Sherman Act, 76 Antitrust L.J. 205 (2009).

The main alternative that has been proposed is a standalone nondiscrimination regime. One such proposal would create a new tribunal to assess innovation harms under a new nondiscrimination standard.[670] The idea is modeled after a tribunal created by the 1992 Cable Act, a forum that adjudicates discrimination complaints against vertically integrated cable video operators pursuant to Section 616 of the Cable Act.[671] If applied to dominant digital platforms, edge innovators alleging discrimination by a dominant platform could file a complaint in the tribunal.[672] Drawing from the cable example, Kevin Caves and Hal Singer observe that the specialized tribunal has resolved discrimination claims in half the time it takes on average to adjudicate a Section 2 antitrust claim in federal court.[673]

In contrast with a separations regime, this proposal institutes a remedy ex post rather than ex ante and through case-by-case adjudication rather than a prophylactic rule.[674] In particular, the complainant bears the burden of showing (1) that its network is similarly situated to the cable operator's affiliated network(s); (2) that it received unfavorable treatment owing to its lack of affiliation as opposed to some efficiency justification; and (3) as a result of (1) and (2) it was materially impaired in its ability to compete effectively. When considering the likely efficacy of such a tribunal in resolving discrimination, it is important to consider its administrability.

For one, the proposal assumes that third-party innovators can identify when they are the subject of discrimination or appropriation. While this may be true in the cable context—where getting blocked or relegated to a less penetrated tier is relatively easy to detect—digital platforms can discriminate in highly subtle ways.[675] While well-resourced incumbents may have the resources to hire experts to identify and investigate discrimination and satisfy the evidentiary burden at a hearing, most small- and medium-sized entrepreneurs will be less able to detect and verify discrimination.

Second, the tribunal approach adopts a quasi-contractual frame, assuming that platforms and edge companies are equal parties to a transaction. This assumption is at odds with the significant asymmetry of power between dominant platforms and the producers that depend on them to get to market. In other words, the fact that bringing discrimination claims would require

---

670. See Caves & Singer, supra note 292, at 20–27 (outlining this proposal).

671. Id. at 21.

672. Id.

673. Id. at 26 (comparing the average duration of each process and concluding that "to the extent that these measures capture the difference between adjudicating a discrimination complaint at the proposed tribunal and in an antitrust court, the duration of adjudication prior to appeal could be reduced by nearly 50 percent").

674. This assumes that separations would be implemented through a statute or rulemaking, rather than as an antitrust remedy.

675. See, e.g., Benjamin Edelman, Mastering the Intermediaries, Harv. Bus. Rev. (June 2014), https://hbr.org/2014/06/mastering-the-intermediaries [https://perma.cc/3AZ2-XNV9] (noting that "[p]latform providers usually get away with relatively subtle discrimination as long as consumers don't notice or care" and describing how Google deprioritized Yelp search results after its proposed acquisition of Yelp fell through).

independent developers or producers to challenge their biggest business partner[676] makes it even less likely that third parties would freely use the tribunal, given potential risks of retaliation.[677] More generally, the tribunal assumes some base level of resources: Independent edge companies without resources would have to depend on the deterrent effect from private enforcement by those with means to avail themselves of the protections. The universe of merchants, developers, and content producers that rely on a dominant platform to reach market is far more numerous and diverse than the universe of cable video programmers that could rely on the tribunal to adjudicate discrimination claims, suggesting that the remedy that works in the cable context may be inapt for the digital platform context.[678]

Moreover, even disputes between well-heeled corporations can take years to resolve. For example, in 2011 Bloomberg filed a complaint with the FCC, alleging that Comcast was improperly grouping Bloomberg's channel in an unfavorable cluster of channels.[679] Since the FCC had conditioned Comcast's acquisition of NBC on the basis of fair "neighborhooding" of independent news networks, Bloomberg claimed that Comcast was in violation of its commitments.[680] Granted that this dispute was adjudicated outside the auspices of section 616 and the agency's ALJ, the FCC took over two years to reach a final decision.[681] Given the importance of timeliness in high-tech markets—where a slight delay can render a remedy obsolete—even a two-year process in digital markets will likely come at the expense of innovation.

In short, while a nondiscrimination regime coupled with a separations remedy would target the platform's incentive and ability to discriminate—be it through integration or through contract—a standalone nondiscrimination remedy would risk being ineffective. For example, the European Commission's remedy in the Google Shopping case—which required Google to implement a nondiscrimination approach—has not changed the underlying market dynamic, prompting content producers to describe it as "neither compliant nor effective."[682]

---

676. See Dzieza, supra note 41 (describing how reliant many merchants are on Amazon's infrastructure).

677. Cf. Jack Nicas, Google Pulls YouTube from Amazon Devices in Retaliation, MarketWatch (Dec. 6, 2017), https://www.marketwatch.com/story/google-pulls-youtube-from-amazon-devices-in-retaliation-2017-12-06 [https://perma.cc/UW32-G9VN] (describing how Google blocked access to YouTube on Amazon devices in retaliation for Amazon's refusal to stock products that compete with its own, "like the Google Home smart speaker or Google's Chromecast streaming device").

678. See, e.g., Dzieza, supra note 41 (describing the diverse merchants on Amazon). Amazon's Marketplace alone has over six million merchants. Id.

679. See Bloomberg L.P. v. Comcast Cable Commc'ns, 28 FCC Rcd. 14,346, 14,347, para. 3 (2013) (noting that Bloomberg filed its complaint on June 13, 2011).

680. Id. at 14,347–49, paras. 3–6 (explaining the background merger between Comcast and NBC, as well as the dispute between Bloomberg and Comcast).

681. See id. at 14,346.

682. Letter from Fourteen European Comparison Shopping Services to Margrethe Vestager, Comm'r for Competition, European Comm'n (Nov. 22, 2018),

A remedy that was more attuned to the significant asymmetry in leverage would not rely entirely on third parties to contest the very intermediary on which their business often depends. Imposing a structural separation—that targets the underlying incentive to discriminate—would mitigate these shortcomings.

CONCLUSION

A handful of digital platforms enjoy increasing control over key arteries of online commerce and communications. How lawmakers and regulators should respond to this concentration of market power is now the subject of a global debate. Public authorities around the world are studying digital platforms to understand how antitrust and competition tools can be applied to markets mediated by digital technologies.[683] These studies vary slightly in their methods and conclusions, but they generally demonstrate that digital platform markets today are governed neither by real competition nor regulation—giving dominant platforms astounding power to shape market outcomes.

In the United States, the process of exploring how to respond to dominant platforms has been stunted by the fact that we are living through a major regulatory gap. The abandonment of traditional regulatory tools in favor of antitrust—followed by the partial collapse of antitrust—has left us with a diminished sense of the policy levers available to address dominant network intermediaries. This Article joins an emerging field of scholarship that is responding to this sense of impoverishment by exploring how traditional principles of economic regulation may apply in the digital age.

The process of identifying how to confront the challenges posed by dominant platforms requires, first, an understanding of the relevant problems and, second, an understanding of the relevant set of legal tools and principles available to confront them. Recovering our understanding of structural separations—traditionally a mainstay regulatory principle for confronting dominant intermediaries—is one part of this process. Reviewing the tradition of separations, moreover, underscores the broader set of values and concerns that traditionally informed how we assessed and arrived at the proper form of intervention when confronted with dominant intermediaries.

Recent events, meanwhile, seem to be driving the public discussion toward separations. Earlier this year, India began enforcing a structural

---

http://www.foundem.co.uk/Comparison_Shopping_Open_Letter_Commissioner_Vestager_Nov_2018.pdf [https://perma.cc/QC9F-EBJM].

683. See, e.g., Australian Competition & Consumer Comm'n, supra note 31, at 7–8 (discussing the anticompetitive risk online platforms pose to Australian consumers, given consumers' "lack of informed and genuine choice" in relying on these platforms); Crémer et al., supra note 3, at 5–7 (summarizing the European Commission's conclusions on the anticompetitive nature of major online platforms); Data Processing in Online Advertising, supra note 31, at 2–10 (providing findings from the French Competition Authority on the dominance that Facebook and Google possess in the market for online advertising); Digital Competition Expert Panel, supra note 31, at 8–16 (providing various recommendations for how the U.K. government can promote competition in digital markets).

separation on foreign online retailers—requiring Amazon to separate its private-label business from its marketplace.[684] In March, Senator Elizabeth Warren rolled out, through her presidential campaign, a proposed separations regime for dominant tech platforms, even drawing support from some tech workers.[685]

Getting the policy right will require careful case-by-case analysis and further study to assess the relevant tradeoffs. Arriving at the proper set of interventions, however, requires first knowing the full set of available tools. Recognizing the tradition of structural separations helps recover not just a mainstay regulatory principle, but also a broader framework for diagnosing and addressing the set of problems that stem from integration by critical gatekeepers.

---

684. See Sankalp Phartiyal, Walmart, Amazon Scrambling to Comply with India's New E-Commerce Rules, Reuters (Jan. 31, 2019), https://www.reuters.com/article/us-india-ecommerce/walmart-amazon-scrambling-to-comply-with-indias-new-e-commerce-rules-idUSKCN1PP1PN [https://perma.cc/3HZR-ES45] ("Another rule blocks entities in which an e-commerce firm, or any of its group companies, owns a stake from selling its products on that firm's marketplace.").

685. See Elizabeth Warren, Here's How We Can Break Up Big Tech, Medium (Mar. 8, 2019), https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c [https://perma.cc/MRX5-5WZY] (proposing "passing legislation that requires large tech platforms to be designated as 'Platform Utilities' and broken apart from any participant on that platform"); see also Casey Tolan, Google, Facebook, Amazon and Apple Employees Donating to Elizabeth Warren, Even Though She Wants to Break Up Big Tech, Mercury News (Apr. 19, 2019), https://www.mercurynews.com/2019/04/19/elizabeth-warren-president-tech-campaign-donations-berine-sanders-kamala-harris/ ("I see a lot of people start companies and their whole plan for the company is to get acquired. . . . It creates this narrow environment where you're only trying to please Facebook or Apple or Google, and I think that is ultimately bad for our country." (internal quotation marks omitted) (quoting Justin Kruger, a freelance software developer)).

APPENDIX. WHY WOULD PLATFORMS UNDERMINE THEIR ECOSYSTEM?

At first glance, the idea that dominant digital platforms may be using their integrated structure to undermine dynamic efficiency appears in tension with standard economic theory. This Appendix examines how to square digital platforms' conduct with an economic understanding of integration in adjacent markets.

Vertical relationships, including full integration, can deliver certain benefits.[686] Integration can help resolve contractual holdup problems that can arise in economically interdependent relationships.[687] It can also reduce costs: Since each company in a vertical transaction usually charges consumers a markup above marginal cost, vertical integration can eliminate this "double marginalization."[688] Moreover, by granting a single firm greater control over quality and interoperability, integration can also better guarantee a stable ecosystem in which platforms and complementary products work together smoothly.[689]

Vertical restraints can also be anticompetitive. Economic literature extensively documents how vertical relationships can raise rivals' costs or deny rivals scale, enable exclusion, or facilitate tacit collusion.[690] When assessing the

---

686. While the focus of this Article is full vertical ownership, other vertical arrangements include joint ventures, tie-ins, long-term contracts, and affiliates.

687. See Bork, Antitrust Paradox, supra note 267, at 226–33; Christopher S. Yoo, Vertical Integration and Media Regulation in the New Economy, 19 Yale J. on Reg. 171, 262–64 (2002). The holdup problems can be especially significant in platform markets, which are commonly characterized as facing a "chicken-and-egg" problem. See David S. Evans, The Antitrust Economics of Two-Sided Markets, 20 Yale J. on Reg. 325, 350 (2003) ("Critical mass . . . is a key start-up issue [for platforms]. Known in the literature as the chicken-and-egg problem, the name does not do the problem justice. In some situations coupled products cannot come into existence without a sufficient number of customers on both sides from the start.").

688. Bork, Antitrust Paradox supra note 267, at 219; see also Joseph J. Spengler, Vertical Integration and Antitrust Policy, 58 J. Pol. Econ. 347, 350 (1950). Notably, evidence today shows that the elimination of double marginalization does not categorically benefit consumers. See, e.g., Fernando Luco & Guillermo Marshall, Vertical Integration with Multiproduct Firms: When Eliminating Double Marginalization May Hurt Consumers 2 (Dec. 7, 2018) (unpublished manuscript), http://ssrn.com/abstract=3110038 (on file with the *Columbia Law Review*) (observing that in multiproduct industries, the elimination of double marginalization caused by vertical integration may cause price changes that hurt consumers).

689. Courts have acknowledged this justification. See United States v. Jerrold Elecs. Corp., 187 F. Supp. 545, 556–57 (E.D. Pa. 1960) (acknowledging that bundling the sale of equipment with engineering services helped "foster the orderly growth of the industry").

690. See, e.g., Oliver Hart & Jean Tirole, Vertical Integration and Market Foreclosure, 1990 Brookings Papers on Econ. Activity 205, 205–07; Thomas G. Krattenmaker & Steven C. Salop, Anticompetitive Exclusion: Raising Rivals' Costs to Achieve Power over Price, 96 Yale L.J. 209, 224 (1986); Patrick Rey & Jean Tirole, A Primer on Foreclosure, *in* 3 Handbook of Industrial Organization 2145, 2148–50 (Mark Armstrong & Robert Porter eds., 2007); Michael H. Riordan, Anticompetitive Vertical Integration by a Dominant Firm, 88 Am. Econ. Rev. 1232, 1232 (1998); Michael A. Salinger, Vertical Mergers and Market Foreclosure, 103 Q.J. Econ., 345, 345–46 (1988); Michael D. Whinston, Exclusivity and Tying in *U.S. v. Microsoft*: What We Know, and Don't Know, 15 J. Econ. Persp. 63, 64 (2001).

competitive implications of vertical acquisitions, enforcers largely assess tradeoffs between foreclosure incentives and claimed reductions in price.

Two theories maintain that integrated firms are unlikely to use their dominant network to discriminate against independent products and services (which are sometimes described in platform literature as "complementors"). Both focus on the incentives faced by an integrated monopolist. Although a monopolist may have the *ability* to discriminate against complementors, these theories hold, the monopolist will generally lack the incentive to do so. It is worth reviewing these economic theories and identifying the exceptions that may explain why dominant platforms appear to engage in this conduct, even in instances in which the platform is not strictly a monopolist.

First, the "single monopoly profit" theory suggests that a monopolist does not have an incentive to discriminate against complementors because it cannot increase its profit by monopolizing a market for complementary products.[691] Say, for example, a monopolist in the bolts market sought also to monopolize the market for nuts. Economic theory holds that there is a single profit-maximizing price for any combination of nuts and bolts, such that raising the price of nuts while maintaining the monopoly-level price of bolts would lead to a decline in demand sufficient to lower total profits. [692] In other words, the bolts monopolist is no better off by also monopolizing nuts. Therefore, the theory goes, the bolts monopolist has nothing to gain by excluding—and thereby driving out—rivals in the nuts market.[693]

The second major explanation for why monopolists lack an incentive to discriminate against complementors is that these independent services may actually raise the monopolist's profits. This "internalizing complementary efficiencies" (ICE) argument holds that if complementors introduce valuable goods or services that generate surplus, the monopolist that hosts these services on its network can capture that surplus.[694] If an operating system with a broader range of applications (or a marketplace with a broader range of products) is more valuable to users than one with a narrower range, then the monopolist has an incentive to cultivate a broader set of complementors. On this view, the

691. Bork, Antitrust Paradox, supra note 267, at 229 ("[A] monopolist has no incentive to gain a second monopoly that is vertically related to the first, because there is no additional monopoly profit to be taken."); Richard A. Posner, Antitrust Law 197–99 (2d ed. 2001); Bowman, supra note 268, at 20–23; Aaron Director & Edward H. Levi, Antitrust Law and the Future: Trade Regulation, 51 Nw. U. L. Rev. 281, 290–92 (1956).

692. 1 Herbert Hovenkamp et al., IP and Antitrust: An Analysis of Antitrust Principles Applied to Intellectual Property Law § 21.03[B] (3d ed. 2018).

693. For explanations relying on a detailed example, see Barbara van Schewick, Internet Architecture, supra note 217, at 222–23 (2010); Einer Elhauge, Tying, Bundled Discounts, and the Death of the Single Monopoly Profit Theory, 123 Harv. L. Rev. 397, 403 (2009) [hereinafter Elhauge, Single Monopoly Profit Theory].

694. Van Schewick, Internet Architecture, supra note 217, at 223; Joseph Farrell & Philip J. Weiser, Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age, 17 Harv. J.L. & Tech. 85, 89 (2003).

monopolist's incentives are aligned with the user's.[695] Not only does the monopolist lack an incentive to exclude valuable complementors[696] but doing so may even lower its profits.[697] ICE explains why it is assumed that a platform monopolist will be a "good steward" of the applications and products that seek access to its platform.[698]

Subsequent learning and research has led scholars to refine both of these theories. While the single monopoly profit idea was initially introduced as a general rule, scholars have since understood that it provides definitive answers under a relatively narrow set of condition.[699] Today the theory is understood to be decisive only when: (1) the monopolist is both unregulated and protected by prohibitive entry barriers, (2) the monopolist's product is used in fixed proportion with the product sold in the adjacent market, and (3) the adjacent market is perfectly competitive.[700] When any of these conditions does not hold, the welfare effects of integration are far more ambiguous. Single monopoly profits, it turns out, are "the exception, not the rule."[701]

Similarly, the assumption that a monopoly platform will always make its platform available whenever it is efficient to do so does not always hold.[702] There are several circumstances under which a platform can be expected to engage in exclusionary conduct that is inefficient.[703] Broadly, a dominant

---

695. See Joseph Farrell, Open Access Arguments: Why Confidence Is Misplaced, *in* Net Neutrality or Net Neutering: Should Broadband Internet Services Be Regulated? 195, 198 (Thomas M. Lenard & Randolph J. May eds., 2003) ("ICE asserts that if a platform sponsor does, or allows to be done, anything that reduces customer value from applications, say by $1, then the demand curve for platform subscription falls by that $1, lowering platform profits by $1 per customer.").

696. See van Schewick, Internet Architecture, supra note 217, at 223 ("Whether the presence of independent producers generates additional surplus depends on consumers' preferences, as well as on such things as the intensity of competition and the degree of differentiation in the complementary market . . . .").

697. See id. at 225 ("Whereas the 'one monopoly rent' theory argues that exclusionary conduct in the complementary market will not increase the monopolist's profits, the 'internalizing complementary efficiencies' theory suggests that such conduct may even reduce its profits.").

698. Farrell & Weiser, supra note 694, at 104.

699. See, e.g., Elhauge, Single Monopoly Profit Theory, supra note 693, at 404 ("However, the model indicating a single monopoly profit depended on several key assumptions . . . . As the economic literature shows, different results are reached if one relaxes these narrow assumptions. Indeed, relaxation of any one of these assumptions produces a distinctive profit-increasing effect."); see also Salop, supra note 272, at 1968–69 (2018) ("This theory is simple but invalid in all but the following extreme conditions . . . .").

700. Salop, supra note 272, at 1968–69; see also Elhauge, Single Monopoly Profit Theory, supra note 693, at 404.

701. Elhauge, Single Monopoly Profit Theory, supra note 693, at 400.

702. The number of exceptions to both the single monopoly profit theorem and ICE has prompted some to question whether these ideas should still be considered general principles. See, e.g., Farrell, supra note 695, at 197 ("However, post-Chicago economics finds that [the one monopoly rent theorem]/ICE has many holes, perhaps too many to be a 'theorem.'").

703. See Farrell & Weiser, supra note 694, at 105–119 (identifying and discussing eight exceptions to ICE); van Schewick, Internet Architecture, supra note 217, at 225–81 (discussing exceptions to the one monopoly rent theorem and ICE).

platform can be expected to engage in exclusionary conduct when (1) it is able to more fully exploit its existing market power or (2) it is able to achieve additional market power.

It is worth briefly identifying the contexts under which these conditions are likely to arise in digital markets.[704]

A. *More Fully Exploiting Existing Market Power: Exclusionary Conduct Enables Price Discrimination*

First, a dominant platform may have an incentive to exclude complementors from its network when doing so would enable it to price discriminate.[705] Price discrimination—or charging customers different prices based on their willingness to pay—enables a monopolist to more fully exploit its existing market power by extracting more consumer surplus.[706] In order to engage in price discrimination, a seller must enjoy some market power—namely, the ability to profitably set price above marginal costs.[707]

Foreclosing or discriminating against certain applications or services can enable the platform to separate consumers into different groups, based on their willingness to pay.[708] For example, the platform can offer different tiers of service: a basic version that provides access to the network but excludes certain applications and a premium version that provides access to the network as well as all applications.[709]

This form of price discrimination may or may not undermine the static welfare of consumers.[710] Analyzing the welfare effects of any price discrimination scheme requires empirical analysis based on consumer preferences and the market's cost structure.[711] But insofar as price discrimination lowers the profits available to complementors, it can depress their incentive to

---

704. Notably, the exceptions reviewed do not assume that only a *monopoly* platform can undermine competition in an adjacent market. Although most of the literature analyzing the exclusionary potential of vertical conduct takes monopoly power to be an "indispensable precondition" for anticompetitive effects, even platforms facing limited competition may have the ability and incentive to exclude competing content, services, or applications. See, e.g., van Schewick, Internet Architecture, supra note 217, at 255 ("A monopoly in the primary market is therefore considered an indispensable precondition for successful monopolization of the secondary market."); id. at 256 ("A network provider may have the ability and incentive to exclude rival content, applications, or portals from its network, even if it faces limited competition in the market for Internet services." (footnote omitted)).

705. See id. at 275–77; Farrell & Weiser, supra note 694, at 107–09.

706. Van Schewick, Internet Architecture, supra note 217, at 275–76.

707. Id. at 276.

708. See id. at 275–76.

709. Id. at 276.

710. See Farrell & Weiser, supra note 694, at 108 ("Price discrimination need not in itself be inefficient or anti-consumer . . . .").

711. See generally Hal R. Varian, Price Discrimination, *in* 1 Handbook of Industrial Organization 597 (Richard Schmalensee & Robert D. Willig eds., 1989) (providing a theoretical background for analyzing the welfare effects of price discrimination).

invest and innovate—thereby undermining dynamic efficiency.[712] More generally, discriminatory pricing can "introduce distortion into the overall market" by "disadvantaging certain classes" of complementors and decreasing the profits available to them by diverting more consumer surplus to the dominant platform.[713]

B. *Expanding Market Power: Complementary Market Is a Source of Outside Revenue*

In the standard economic model, a monopolist in the primary market is assumed to capture its entire monopoly profit from that market, limiting its ability to earn a second monopoly profit.[714] But if firms in the complementary market derive revenue from other sources—such as advertising—then the monopolist in the primary market will likely have an incentive to monopolize the secondary market as well.[715] Since excluding rivals in the complementary market can diminish for consumers the value of the primary network, the overall gains in outside revenue postexclusion will need to be greater than the profit reduction in the primary-good market in order for exclusion to be a profitable strategy.[716]

Digital platforms that operate in distinct but interrelated markets are likely to fit this exception. Google, for example, provides its search engine at zero monetary price and earns the vast majority of its net income through selling digital ad placement.[717] When considering whether to grant third-party content providers equal access to its search platform, Google must weigh the revenue it could lose through discriminating against third-party content[718] against the revenue it could gain through monopolizing the secondary market. Privileging its own content sites would help keep users within the Google ecosystem, which would in turn allow Google both to capture greater user data and to sell more (and potentially higher-priced) ads.[719] Given that behavioral ad markets

712. See van Schewick, Internet Architecture, supra note 217, at 277–78; Wu, Network Neutrality, supra note 16, at 153; see also Farrell & Katz, supra note 199, at 414 ("[F]irm M's desire and ability to extract rents from independent suppliers *after* they have conducted their R&D may inefficiently reduce these suppliers' innovation incentives . . . .").

713. Van Schewick, Internet Architecture, supra note 217, at 277.

714. See id. at 222–23.

715. See id. at 233.

716. Id.

717. See 2018 Alphabet 10-K, supra note 106, at 4–5, 27.

718. Since Google does not charge a monetary price for using its search engine, calculating the revenue loss that results from one user abandoning Google Search is not straightforward. Since Google monetizes the user through selling ads, see id. at 4–5, 27, the revenue loss would be on the ad side.

719. Notably, this does not assume or require that Google capture the secondary market. See van Schewick, Internet Architecture, supra note 217, at 237 ("Even without monopolizing a specific market in which advertisers buy access to the network provider's Internet customers, selling access to a large block of customers may be more profitable than selling access to subgroups of that block.").

place a premium on comprehensive user data,[720] prioritizing Google verticals in Google search results is likely to be lucrative. Whether this exclusionary conduct would offset potential revenue losses to Google's primary network is an empirical question.

More generally, it is worth examining whether certain features exhibited by digital platform markets may change the default calculus in *favor* of exclusion. If a standard choice faced by a dominant platform is whether to grant rival complementors access to its network and charge a fee to extract some of their revenue or to exclude all rival complementors and sell the service itself, then digital markets seem to tip the balance in favor of the latter. This is because digital platforms are making an ecosystem play: By bundling different services and portals, a platform can heighten switching costs and collect more user data by tracking individuals across services, both of which amount to a lucrative strategy.[721] The enormous value assigned to user datasets suggests that platforms will have an even greater incentive to keep users within their walled gardens, meaning that they will be more likely to choose direct access and exclusion over shared access and complementor revenue.

Lastly, online markets may lower the cost of exclusion. While foreclosure strategies traditionally involve denying a third-party access outright, digital markets enable subtler forms of discrimination.[722] Discriminating against a complementor risks increasing user dissatisfaction with the product, but users will have limited insight into the source of the quality degradation, reducing the chance that they will respond by abandoning the platform. In other words, if Apple denies Spotify upgrades on iOS, users may blame Spotify rather than Apple, limiting Apple's exposure to users abandoning Apple. Switching costs, moreover, can be significant in digital platform markets, especially in the absence of interoperability or data portability regimes—a fact that also reduces the cost of exclusion.[723]

---

720. See Newman, Control of User Data, supra note 286, at 407 (noting that Google's "integrated profile[s]" of its users are valuable to advertisers).

721. See id. (noting that Google's many products and services "allow[] it to develop an integrated profile of more individuals," which it then uses "to allow advertisers to more effectively target particular ads").

722. See van Schewick, Internet Architecture, supra note 217, at 260 ("[T]he network provider may be able to engage in exclusionary conduct without losing too many of its Internet-service customers by using discrimination instead of direct exclusion."). For example, instead of blocking access to a complementary product, a network provider could merely slow that complementary product—a subtler form of discrimination that the network provider's internet-service customers would be less likely to notice. See id.

723. See Adam Candeub, Behavioral Economics, Internet Search, and Antitrust, 9 I/S: J.L. & Pol'y for Info. Soc'y 407, 409 (2014) ("If we establish habits and routines to allocate our scarce cognitive resources, these routines—like many other habits—can be quite difficult, *i.e.*, costly, to break, creating high switching costs with possible anti-competitive implications."); Newman, Digital Markets, supra note 579, at 8–12, 20 (discussing various factors that lead to high switching costs in digital markets).

C. *Expanding Market Power: Primary Good Is Inessential for Uses of Complementary Good*

Another set of conditions under which a dominant platform will have an incentive to foreclose rivals in a complementary market occurs when: (1) the dominant platform's complementary good can be used independently of the primary platform, (2) the platform can stop its competitors from selling their version of the complementary good to the platform's users, and (3) the complementary market exhibits economies of scale or network effects.[724]

Because a platform monopoly facing these conditions would not be able to extract all monopoly profits through its pricing of the primary service, it would have an incentive to extend its monopoly into the complementary market.[725] The existence of network effects, meanwhile, enables the monopolist to thwart potential rivals from the complementary market by excluding them from the primary market.[726]

Even if the platform is not a monopolist, exclusionary conduct that drove more sales of the complementary good or service would likely be profitable. Because the cost structure of applications and content usually involves high fixed costs and low marginal costs, any subsequent sales—presumably at prices above marginal cost—would likely generate profits.[727]

724. See van Schewick, Internet Architecture, supra note 217, at 226–27.

725. See id. at 227.

726. See id.

727. See id. at 252.

Chapter 34

A Skeptical View of Information Fiduciaries (Lina M. Khan and David E. Pozen)

Draft of May 25, 2019

A Skeptical View of Information Fiduciaries

Lina M. Khan[*] & David E. Pozen[**]

The concept of "information fiduciaries" has surged to the forefront of debates on online platform regulation. Developed by Professor Jack Balkin, the concept is meant to rebalance the relationship between ordinary individuals and the digital companies that accumulate, analyze, and sell their personal data for profit. Just as the law imposes special duties of care, confidentiality, and loyalty on doctors, lawyers, and accountants vis-à-vis their patients and clients, Balkin argues, so too should it impose special duties on corporations such as Facebook, Google, and Twitter vis-à-vis their end users. Over the past several years, this argument has garnered remarkably broad support and essentially zero critical pushback.

This Essay seeks to disrupt the emerging consensus by identifying a number of lurking tensions and ambiguities in the theory of information fiduciaries, as well as a number of reasons to doubt the theory's capacity to resolve them satisfactorily. Although we agree with Balkin that the harms stemming from dominant online platforms call for legal intervention, we question whether the concept of information fiduciaries is an adequate or apt response to the problems of information insecurity that he stresses, much less to more fundamental problems associated with outsized market share and business models built on pervasive surveillance. We also call attention to the potential costs of adopting an information-fiduciary framework—a framework that, we fear, invites an enervating complacency toward online platforms' structural power and a premature abandonment of more robust visions of public regulation.

[*] Academic Fellow, Columbia Law School.

[**] Professor of Law, Columbia Law School. For helpful comments and conversations, we thank Alex Abdo, Jack Balkin, Lauren Beck, Danielle Citron, Evan Criddle, Niki Edmonds, Andrew Gold, James Grimmelmann, Claudia Haupt, Thomas Kadri, Amy Kapczynski, Ramya Krishnan, Ronald Krotoszynski, Genevieve Lakier, Ethan Leib, Barry Lynn, Tamara Piety, Robert Post, Jed Purdy, Neil Richards, Marc Rotenberg, Chuck Sabel, Ganesh Sitaraman, Matt Stoller, Tim Wu, and Jonathan Zittrain, as well as workshop participants at Cornell Tech, University of Maryland School of Law, and Yale Law School.

INTRODUCTION

Digital businesses such as Facebook, Google, and Twitter collect an enormous amount of data about their users. Sometimes they do things with this data that threaten the users' best interests, from allowing predatory advertising and enabling discrimination to inducing addiction and sharing sensitive details with third parties. Online platforms may also disserve their users and the general public in myriad other ways, including by facilitating the spread of disinformation and the harassment of certain categories of speakers. The European Union has responded to some of these concerns with a comprehensive personal data law, the General Data Protection Regulation (GDPR).[1] After years of relative neglect, U.S. policymakers, roused by Russian interference in the 2016 presidential election and the Facebook–Cambridge Analytica scandal, have begun to consider a range of reforms to enhance consumer privacy, corporate transparency, and data security on the internet.[2] To an unprecedented degree, technology firms in general and online platforms in particular find themselves "in Congress's sights."[3]

Among the reforms under consideration is the idea of treating online platforms as "information fiduciaries." Professor Kenneth Laudon appears to have coined this phrase in the early 1990s.[4]

[1] Council Regulation 2016/679, 2016 O.J. (L 119). The GDPR, which was adopted in 2016 and entered into force in May 2018, replaces a 1995 directive on data protection, Council Directive 95/46, 1995 O.J. (L 281).

[2] *See, e.g.*, Senator Mark R. Warner, Potential Policy Proposals for Regulation of Social Media and Technology Firms (2018), https://graphics.axios.com/pdf/PlatformPolicyPaper.pdf (surveying policy options).

[3] Heather Whitney, *Search Engines, Social Media, and the Editorial Analogy*, KNIGHT FIRST AMEND. INST. 2 (2018), https://knightcolumbia.org/sites/default/files/content/Heather_Whitney_Search_Engines_Editorial_Analogy.pdf.

[4] *See* Kenneth C. Laudon, *Markets and Privacy*, *in* ICIS 1993 PROCEEDINGS 65, 70–71 (1993) (proposing a "National Information Market" within which "information fiduciaries would . . . accept

Since 2014, it has been identified with Professor Jack Balkin, who has developed the idea over a series of papers.[5] Ordinary people, Balkin observes, are deeply dependent on and vulnerable to the digital companies that accumulate, analyze, and sell their personal data for profit. To mitigate this vulnerability and ensure these companies do not betray the trust people place in them,[6] Balkin urges that we draw on principles of fiduciary obligation. Just as the law imposes special duties of care, confidentiality, and loyalty on doctors, lawyers, accountants, and estate managers vis-à-vis their patients and clients, so too should it impose such duties on Facebook, Google, Microsoft, Twitter, and Uber vis-à-vis their end users—although Balkin concedes that the duties will be "more limited" in the digital context.[7]

Support for this idea is swelling. Dozens of legal scholars have endorsed Balkin's proposal or discussed it approvingly.[8] Journalists have covered it with undisguised enthusiasm; a recent

---

deposits of information from depositors and seek to maximize the return on sales of that information in national markets or elsewhere in return for a fee").

[5] Balkin first promoted the idea in a 2014 blog post. Jack Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [hereinafter Balkin, *Digital Age*]. He most fully elaborated his views in Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) [hereinafter Balkin, *Information Fiduciaries*]. Additional discussions include Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1160–63 (2018) [hereinafter Balkin, *Algorithmic Society*]; Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2047–55 (2018) [hereinafter Balkin, *Triangle*]; Jack M. Balkin, *Fixing Social Media's Grand Bargain* 11–15 (Hoover Inst., Aegis Paper No. 1814, 2018), https://www.hoover.org/sites/default/files/research/docs/balkin_webreadypdf.pdf [hereinafter Balkin, *Fixing Social Media*]; and Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346. Professor Jonathan Zittrain has also been an important theorist and advocate of the information-fiduciary concept. *See, e.g.*, Balkin & Zittrain, *supra*; Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering; Jonathan Zittrain, *How to Exercise the Power You Didn't Ask For*, HARV. BUS. REV. (Sept. 19, 2018), https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for [hereinafter Zittrain, *How to Exercise*]; Jonathan Zittrain, *Mark Zuckerberg Can Still Fix This Mess*, N.Y. TIMES (Apr. 7, 2018), https://www.nytimes.com/2018/04/07/opinion/sunday/zuckerberg-facebook-privacy-congress.html [hereinafter Zittrain, *Fix This Mess*].

[6] In recent years, a number of privacy law scholars have highlighted ways in which privacy and trust are intertwined online, if not co-constitutive. *See generally, e.g.*, ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2018).

[7] Balkin, *Information Fiduciaries*, *supra* note 5, at 1226; Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1229 (2017) [hereinafter Balkin, *Three Laws of Robotics*]; Balkin, *Fixing Social Media*, *supra* note 5, at 12.

[8] On our reading, the academic literature taking up the idea of information fiduciaries has been overwhelmingly supportive. For representative responses from leading scholars of internet law, see Frank Pasquale, *Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society*, 78 OHIO ST. L.J. 1243, 1244 (2017) ("I believe that Balkin's concept of information fiduciary is well developed and hard to challenge."); Tim Wu, *An American Alternative to Europe's Privacy Law*, N.Y. TIMES (May 30, 2018), https://www.nytimes.com/2018/05/30/opinion/europe-america-privacy-

Bloomberg subheadline reads: "America needs data rules that won't crush the tech industry. One law professor may have figured out a solution."[9] Lawmakers from both parties have expressed interest.[10] This past December, a group of fifteen Democratic Senators took the next step and introduced legislation that would require online service providers to act as fiduciaries for their users, drawing directly from Balkin's proposal.[11] Facebook CEO Mark Zuckerberg has now signaled his support as well.[12] Balkin is the legal academy's preeminent diagnostician of how

gdpr.html ("[Social media] companies should be considered, to borrow a term coined by the law professor Jack Balkin, 'information fiduciaries' . . . ."). The closest we have found to a skeptical note is Professor Jane Bambauer's suggestion that an "*expansion* of Balkin's proposal" to cover additional classes of data collectors, such as Netflix and Amazon, "could cause unsettling distortions of free speech protection." Jane R. Bambauer, *The Relationships Between Speech and Conduct*, 49 U.C. DAVIS L. REV. 1941, 1949 (2016) (emphasis added). As far as we are aware, this Essay is the first to apply any sustained critical scrutiny to the information-fiduciary concept.

[9] Editorial, *How to Make Facebook and Google Behave*, BLOOMBERG (Apr. 24, 2018), https://www.bloomberg.com/opinion/articles/2018-04-24/make-facebook-and-google-information-fiduciaries [hereinafter Bloomberg Editorial]. On a single day this past spring, Balkin's proposal received glowing coverage in multiple popular pieces. *See* Russell Brandom, *This Plan Would Regulate Facebook Without Going Through Facebook*, VERGE (Apr. 12, 2018), https://www.theverge.com/2018/4/12/17229258/facebook-regulation-fiduciary-rule-data-proposal-balkin; Yves Faguy, *Regulating Facebook to Make It an Information Fiduciary*, NAT'L (CAN. BAR ASS'N) (Apr. 12, 2018), https://web.archive.org/web/20180416050935/http://www.nationalmagazine.ca/Articles/April-2018/Regulating-Facebook-to-make-it-an-information-fidu.aspx; Nathan Heller, *We May Own Our Data, but Facebook Has a Duty to Protect It*, NEW YORKER (Apr. 12, 2018), https://www.newyorker.com/tech/annals-of-technology/we-may-own-our-data-but-facebook-has-a-duty-to-protect-it.

[10] *See, e.g.*, 164 CONG. REC. S2026 (daily ed. Apr. 10, 2018) (statement of Sen. John Cornyn) ("Perhaps we should treat social media platforms as information fiduciaries and impose legal obligations on them, as we do with lawyers and doctors, who are privy to some of our most personal, private information."); Warner, *supra* note 2, at 14–15 (listing Balkin's idea first on a list of policy options for Congress to consider in the area of "Privacy and Data Protection"); Heller, *supra* note 9 (observing that "[t]o a striking degree, the fiduciary model was the one toward which discussion . . . converged" in an April 2018 Senate hearing on Facebook); *see also* Zittrain, *How to Exercise*, *supra* note 5 ("We've found that our [information-fiduciary] proposal has bipartisan appeal in Congress . . . .").

[11] Data Care Act of 2018, S. 3744, 115th Cong. (2018); *see also* Press Release, Office of Sen. Brian Schatz, Schatz Leads Group of 15 Senators in Introducing New Bill to Help Protect People's Personal Data Online (Dec. 12, 2018), https://www.schatz.senate.gov/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online (describing the proposed legislation, referred to as the "Data Fiduciary Act" by Senator Cory Booker, as "establishing a fiduciary duty for online providers").

[12] When Senator Brian Schatz, a lead sponsor of the Data Care Act, raised Balkin's information-fiduciary idea at a high-profile hearing last year, Zuckerberg "seemed to perk up." Brandom, *supra* note 9. "'I think it's certainly an interesting idea,' Zuckerberg said, 'and Jack is very thoughtful in this space, so I do think it deserves consideration.'" *Id.* At a more recent event with Zittrain, Zuckerberg described the "idea of [Facebook] having a fiduciary relationship with the people who use our services" as "intuitive" and consistent with Facebook's "own self-image . . . and what we're doing." *At Harvard Law, Zittrain and Zuckerberg Discuss Encryption, 'Information Fiduciaries' and Targeted Advertisements*, HARV. L. TODAY (Feb. 20, 2019), https://today.law.harvard.edu/at-harvard-law-zittrain-and-zuckerberg-discuss-encryption-information-fiduciaries-and-targeted-advertisements [hereinafter *Zittrain and Zuckerberg*].

theories can move over time from the margins to the mainstream, from "off the wall" to "on the wall."[13] He is also an ingenious idea entrepreneur whose own theory of information fiduciaries is rapidly making this very transition.

We admire Balkin's ingenuity and applaud his efforts to advance the cause of platform regulation. Yet while we largely agree with his analysis of *why* certain digital firms should be regulated more vigorously, we question whether the concept of information fiduciaries is an adequate or apt response to the problems of information asymmetry and abuse that he stresses, much less to more fundamental problems associated with outsized market share and business models that demand pervasive surveillance. The primary aims of this Essay are, first, to identify a number of lurking ambiguities and tensions in the theory of information fiduciaries and, second, to raise concerns about the theory's capacity to resolve them satisfactorily.[14] The Essay also calls attention to the potential costs of adopting an information-fiduciary framework—a framework that, we fear, invites an enervating complacency about issues of structural power and a premature abandonment of more robust visions of public regulation.

I. FIDUCIARIES FOR WHOM?

Balkin offers his theory of information fiduciaries as a response to problems of asymmetric vulnerability and dependency online. A key feature of the digital economy, he observed in his original essay on the subject, is that "[m]any of the online services that people use require them to trust companies with sensitive personal information."[15] These companies have "increasing capacities for surveillance and control" of their users, but users have little ability to monitor the companies.[16] Users therefore worry, with good reason, that the companies will take advantage of them. To help level the playing field and allay such worries, Balkin proposes that we draw on principles of fiduciary law that assign one actor (the fiduciary) "special obligations of loyalty and trustworthiness" toward another actor (the beneficiary).[17] As Balkin emphasizes, fiduciary relationships have been created in a variety of contexts, including where ordinary individuals

[13] *See, e.g.*, JACK M. BALKIN, CONSTITUTIONAL REDEMPTION 12, 61, 69–70, 88, 119, 177–83 (2011); Jack M. Balkin, *From Off the Wall to On the Wall: How the Mandate Challenge Went Mainstream*, THE ATLANTIC (June 4, 2012), http://www.theatlantic.com/national/archive/2012/06/from-off-the-wall-to-on-the-wall-how-the-mandate-challenge-went-mainstream/258040.

[14] Given that the firms Balkin would designate as information fiduciaries vary in the services they provide, the business models they use, and the market dominance they enjoy, any analysis of the designation's appropriateness or helpfulness will necessarily vary to some extent by firm. For purposes of this analysis, we focus above all on Facebook, both because Facebook is Balkin's main example of a digital information fiduciary and because it is the company whose practices have most galvanized privacy reformers in recent years. Facebook also happens to offer a particularly stark case study in the inadequacies of the information-fiduciary framework.

[15] Balkin, *Digital Age*, *supra* note 5.

[16] Balkin, *Fixing Social Media*, *supra* note 5, at 12; *see also* Balkin, *Algorithmic Society*, *supra* note 5, at 1162 ("End-users are transparent to these organizations, but their operations are not transparent to end-users, and it is difficult if not impossible to monitor their operations.").

[17] Balkin, *Information Fiduciaries*, *supra* note 5, at 1207. Throughout this Essay, we will use "beneficiaries" as a catch-all term for those to whom fiduciary obligations are owed.

surrender sensitive information to a professional expert—such as a doctor, lawyer, or accountant—to obtain the benefit of the fiduciary's valuable-yet-not-fully-comprehensible skills and services.[18]

The principal goal of designating digital companies as fiduciaries for their users, Balkin explains, is to prevent these companies from engaging in "egregious . . . bad behavior."[19] No longer will they be able to act like "con artists."[20] "The long-term goal is to create legal incentives" for the development of "public-oriented" corporate cultures and industry norms.[21] Importantly, Balkin maintains that these goals can be pursued without running afoul of the First Amendment[22] or disrupting "the basic business model of free or subsidized online services" furnished in exchange for the collection and monetization of user data.[23] A fiduciary approach, in the words of Balkin's collaborator Jonathan Zittrain, "protects consumers and corrects a clear market failure without the need for heavy-handed government intervention."[24]

Assessing these claims requires consideration of, among other things, the legal status quo faced by the relevant companies. Start with corporate law.[25] Balkin's central example of a purported information fiduciary, Facebook, is a Delaware corporation.[26] So are his other main examples, Google, Twitter, and Uber.[27] Under Delaware law, the officers and directors of a for-profit corporation already owe fiduciary duties—to the corporation and its stockholders. Although the

[18] *See, e.g.*, Balkin, *Algorithmic Society*, *supra* note 5, at 1160 (discussing the development of fiduciary relationships in settings where a "client relies on the fiduciary to perform valuable services" but "is not well-equipped to understand and monitor the fiduciary's operations").

[19] Balkin, *Fixing Social Media*, *supra* note 5, at 11.

[20] Balkin, *Algorithmic Society*, *supra* note 5, at 1163; Balkin, *Triangle*, *supra* note 5, at 2053; Balkin, *Three Laws of Robotics*, *supra* note 7, at 1229; *see also* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1094–95 (2019) (echoing Balkin's "con men" formulation and surveying how advocates of the information-fiduciary framework have defined the obligations that digital fiduciaries would owe their users).

[21] Balkin, *Fixing Social Media*, *supra* note 5, at 12.

[22] *See infra* section IV.A (reviewing and critiquing this line of argument).

[23] Balkin, *Information Fiduciaries*, *supra* note 5, at 1227.

[24] Zittrain, *How to Exercise*, *supra* note 5.

[25] Part III turns, briefly, to consumer protection and contract law.

[26] *See* Facebook, Inc., Registration Statement (Form S-1) (Feb. 1, 2012) (listing Delaware as Facebook's jurisdiction of incorporation).

[27] *See* Google Inc., Registration Statement (Form S-1) (Apr. 29, 2004); Twitter, Inc., Registration Statement (Form S-1) (Oct. 3, 2013); Uber Technologies, Inc., Restated Certificate of Incorporation (Feb. 28, 2015). Additional companies that Balkin has characterized as information fiduciaries, including Airbnb and OkCupid, are likewise Delaware corporations. *See* Balkin, *Three Laws of Robotics*, *supra* note 7, at 1230; Airbnb, Inc., Notice of Exempt Offering of Securities (Form D) (Mar. 9, 2017); Match Group, Inc., Registration Statement (Form S-1) (Nov. 9, 2015). Microsoft also makes Balkin's list and is incorporated in the state of Washington. *See* Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66 BUFF. L. REV. 979, 1006 (2018) [hereinafter Balkin, *Second Gilded Age*]; Amended and Restated Articles of Incorporation of Microsoft Incorporation (Nov. 24, 2009); *cf.* Shanika Weerasundara, *State of the "Incorporation"—Delaware or Washington?*, TEQLAA (Mar. 16, 2016), http://www.teqlaa.com/state-of-the-incorporation-delaware-or-washington (stating that "Washington corporate law is largely similar to Delaware law" and that "Washington courts often refer to Delaware case law as guidance" in interpreting the Washington Corporation Act).

doctrinal details are complex, the core duty of loyalty is fairly straightforward. As the Court of Chancery explained in 2017, "Delaware case law is clear" that to act loyally, officers and directors "must, within the limits of [their] legal discretion, treat stockholder welfare as the only end, considering other interests only to the extent that doing so is rationally related to stockholder welfare.'"[28] Or put another way: "'Non-stockholder constituencies and interests can be considered, but only instrumentally, . . . when giving consideration to them can be justified as benefiting the stockholders.'"[29] In 2013, Delaware created by statute a new category of corporations, public benefit corporations, whose directors are permitted to "balance[] the pecuniary interests of the stockholders" against "the best interests of those materially affected by the corporation's conduct" and other public values.[30] The creation of this category reinforces the conventional view that Delaware fiduciary law simply "does not permit traditional corporations to consider non-stockholder constituencies."[31]

Right off the bat, these observations give reason to question the feasibility, if not also the coherence, of applying the information-fiduciary idea to the leading social media companies. A fiduciary with sharply opposed loyalties teeters on the edge of contradiction.[32] Insofar as the interests of stockholders and users diverge, the officers and directors of these companies may be

[28] Frederick Hsu Living Trust v. ODN Holding Corp., No. 12108-VCL, 2017 WL 1437308, at *17 (Del. Ch. Apr. 24, 2017) (quoting Leo E. Strine, Jr., *A Job Is Not a Hobby: The Judicial Revival of Corporate Paternalism and Its Problematic Implications*, 41 J. CORP. L. 71, 107 (2015)).

[29] *Id.* at *17 n.14 (quoting Leo E. Strine, Jr., *The Dangers of Denial: The Need for a Clear-Eyed Understanding of the Power and Accountability Structure Established by the Delaware General Corporation Law*, 50 WAKE FOREST L. REV. 761, 771 (2015)); *see also* eBay Domestic Holdings, Inc. v. Newmark, 16 A.3d 1, 34 (Del. Ch. 2010) (stating that Delaware fiduciary principles require directors "to maximize the economic value of a for-profit Delaware corporation for the benefit of its stockholders"); Julian Velasco, *Fiduciary Principles in Corporate Law*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 61, 64 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019) ("In Delaware, at least, . . . a corporate fiduciary's duties ultimately are owed to the shareholders alone.").

[30] Del. Code Ann. tit. 8, § 365(a) (2017) (effective Aug. 1, 2013).

[31] Ellen J. Odoner, Stephen A. Radin, Lyuba A. Goltser & Andrew E. Blumberg, *Fiduciary Duties of Corporate Directors in Uncertain Times*, MILLSTEIN CTR. FOR GLOBAL MARKETS & CORP. OWNERSHIP 4 (2017), https://millstein.law.columbia.edu/sites/default/files/content/docs/105715_millstein_fiduciary_duties.pdf. The extent to which Delaware fiduciary law actually protects shareholders against managerial negligence and self-dealing, compliance failures that result in penalties on the firm, and other bad behavior by corporate officers has been debated for decades. *See generally* Velasco, *supra* note 29, at 62–63 (discussing the many "compromises" made by corporate fiduciary law to conserve legal resources and minimize "interference with risky business decisions"). In her response to this Essay, Professor Tamara Piety contends that Delaware law has not proven an effective deterrent to much of this behavior and that this track record supplies an additional reason for skepticism about Balkin's proposal. Tamara R. Piety, *Radical Skepticism About Information Fiduciaries*, LAW & POL. ECON. [cite].

[32] *Cf.* Paul B. Miller, *Multiple Loyalties and the Conflicted Fiduciary*, 40 QUEEN'S L.J. 301, 303, 306 (2014) (explaining that the fiduciary "right of loyalty is commonly understood as being an *exclusive* claim enjoyed by the beneficiary over the exercise of discretionary power by a fiduciary," but noting that there are some "difficult" cases in which fiduciaries are "authorized to act in the face of a known conflict"). We consider in Part II how some of the standard legal strategies for managing conflicts among classes of beneficiaries might be mapped onto Balkin's proposal.

put in the untenable position of having to violate their fiduciary duties (to stockholders) under Delaware law in order to fulfill their fiduciary duties (to end users) under the new body of law that Balkin proposes—at least barring some sort of "heavy-handed government intervention"[33] that expressly prioritizes the latter set of duties.

It is not hard to imagine how the interests of a social media company's stockholders and users could come apart. We will return to this point in section II.B, but just consider for a moment Facebook's situation. Facebook is primarily a digital advertising venture. It charges users no monetary price for using the platform and instead makes the vast majority of its revenue through selling targeted advertising placements to third parties.[34] Like other corporations with comparable business models, Facebook therefore has a strong economic incentive to maximize the amount of time users spend on the site and to collect and commodify as much user data as possible.[35] By and large, addictive user behavior is good for business.[36] Divisive and inflammatory content is good for business.[37] Deterioration of privacy and confidentiality norms is good for business.[38] Reforms to make the site less addictive, to deemphasize sensationalistic material, and to enhance personal

[33] Zittrain, *How to Exercise*, *supra* note 5.

[34] *See, e.g.*, *Facebook's Annual Revenue from 2009 to 2017, by Segment (in Million U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/267031/facebooks-annual-revenue-by-segment (last visited Feb. 18, 2019) (indicating that over 98 percent of Facebook's total revenue in 2017, nearly $40 billion, came from advertising). This is not true of dating sites or gig economy companies like Uber and Airbnb, which charge customers for services.

[35] As Balkin notes, "advertising revenues depend on the amount of time and attention spent on the site." Balkin, *Fixing Social Media*, *supra* note 5, at 2.

[36] *See generally* ADAM ALTER, IRRESISTIBLE: THE RISE OF ADDICTIVE TECHNOLOGY AND THE BUSINESS OF KEEPING US HOOKED (2017).

[37] *See, e.g.*, Emily Bell & Taylor Owen, *The Platform Press: How Silicon Valley Reengineered Journalism*, TOW CTR. FOR DIGITAL JOURNALISM (Mar. 29, 2017), https://www.cjr.org/tow_center_reports/platform-press-how-silicon-valley-reengineered-journalism.php (explaining that "the structure and the economics of social platforms incentivize the spread of low-quality content over high-quality material"); Sue Halpern, *Apologize Later*, N.Y. REV. BOOKS, Jan. 17, 2019, at 12, 14 ("While the formula [Facebook] came up with was quite simple—growth is a function of engagement—it so happened that engagement was best served by circulating sensational, divisive, and salacious content. Allowing discordant and false material on the platform was not a glitch in the business plan—it was the plan."); Nicholas Thompson & Fred Vogelstein, *Inside the Two Years That Shook Facebook—and the World*, WIRED (Feb. 12, 2018), https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell (discussing the growing recognition after the 2016 presidential election "that Facebook had long helped to create an economic system that rewarded publishers for sensationalism, not accuracy or depth").

[38] *See, e.g.*, BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 1–28 (2015) (discussing Facebook's data-mining and surveillance practices and the degree to which they foster and depend upon "a society of *exposure* and *exhibition*," in which people are "dulled into not caring" about privacy "because there is 'nothing to hide' and 'no place to hide'"); Bruce Schneier, *How We Sold Our Souls—and More—to the Internet Giants*, THE GUARDIAN (May 17, 2015), https://www.theguardian.com/technology/2015/may/17/sold-our-souls-and-more-to-internet-giants-privacy-surveillance-bruce-schneier (explaining, with reference to Facebook, that "[s]urveillance is the business model of the internet" and that people's "tendency to undervalue privacy is exacerbated by companies deliberately making sure that privacy is not salient to users").

privacy would arguably be in the best interests of users. Yet each of these reforms would also pose a threat to Facebook's bottom line and therefore to the interests of shareholders.[39]

Doctors, lawyers, accountants, and the like do not experience such acute tensions within their sets of fiduciary obligations. Tensions do arise, both because these fiduciaries may stand to profit from selling beneficiaries as many products and services as possible (whatever the beneficiaries' true needs) and because there may be misalignments among beneficiaries, as in the case of a financial servicer acting on behalf of multiple investors[40] or a law firm partner with fiduciary duties to her copartners as well as her clients.[41] Some of these fiduciaries may even be employed by publicly traded companies,[42] although most are not; longstanding rules of professional conduct, for instance, prohibit nonlawyer ownership of law firms in the United States.[43] Yet while Delaware law allows for directors' duties to shareholders to be qualified by other legal duties[44] and while digital information fiduciaries would not be unique in facing cross-cutting fiduciary obligations, the nature and scope of the inter-fiduciary conflicts they would face seem qualitatively distinct. As

[39] Recent market developments corroborate this concern. In January 2018, Facebook adjusted its algorithm to favor more content from "friends" and less content from brands and publishers, a move its CEO promoted as ensuring that time spent on the platform is "time well spent." Post of Mark Zuckerberg, Facebook (Jan. 11, 2018), https://www.facebook.com/zuck/posts/10104413015393571. Immediately after Facebook announced that the adjustment had led users to spend less time on the platform, the company's stock fell by five percent, "a rare decline for a company that consistently outpaces Wall Street's estimates." Seth Fiegerman, *Facebook Users Are Spending Less Time on the Site*, CNN (Jan. 31, 2018), https://money.cnn.com/2018/01/31/technology/facebook-earnings/index.html.

[40] *See* Steven L. Schwarcz, *Fiduciaries with Conflicting Obligations*, 94 MINN. L. REV. 1867 *passim* (2010) (discussing this phenomenon); *see also* Kent Greenfield, *New Principles for Corporate Law*, 1 HASTINGS BUS. L.J. 87, 103 (2005) (noting that corporate directors "owe fiduciary duties to holders of all classes of stock even when the interests of the various classes are in conflict").

[41] *See* Robert W. Hillman, *The Impact of Partnership Law on the Legal Profession*, 67 FORDHAM L. REV. 393, 399 (1998) ("A lawyer as fiduciary serves two masters—the lawyer's partners and the lawyer's clients. The differing interests of the beneficiaries of a partner's loyalty obligation may diverge significantly and even be in conflict."); *see also, e.g.*, Raymond T. Nimmer & Richard B. Feinberg, *Chapter 11 Business Governance: Fiduciary Duties, Business Judgment, Trustees and Exclusivity*, 6 BANKR. DEV. J. 1, 27 (1989) (describing how debtor-in-possession fiduciaries bear "not only the obligation to protect the estate, but also the explicit power to make choices that benefit some claimants and harm others").

[42] Numerous companies that own or operate U.S. hospitals are publicly traded, for example. *See Publicly Traded Healthcare Facilities*, INVESTSNIPS (last visited Feb. 18, 2019), http://investsnips.com/list-of-publicly-traded-healthcare-facilities-blood-banks-emergency-rooms-treatment-facilities-and-urgent-care-centers.

[43] *See* Roberta S. Karmel, *Will Law Firms Go Public?*, 35 U. PA. J. INT'L L. 487, 490–91 (2013) (reviewing these rules and explaining that the "basic concern animating [them] is that permitting nonlawyer ownership or direction would subject lawyers to meeting the goals of the nonlawyers rather than meeting their duties to clients"). There has been some debate in recent years about whether these rules should be relaxed, as they have been in several Commonwealth countries, but as of now they still hold. *See generally id.*; Nick Robinson, *When Lawyers Don't Get All the Profits: Non-Lawyer Ownership, Access, and Professionalism*, 29 GEO. J. LEGAL ETHICS 1 (2016); Elizabeth Olson, *A Call for Law Firms to Go Public*, N.Y. TIMES (Feb. 18, 2015), https://dealbook.nytimes.com/2015/02/18/a-call-for-law-firms-to-go-public.

[44] This is the import of the phrase "within the limits of [their] legal discretion" in the passage quoted *supra* note 28 and accompanying text.

Balkin acknowledges, traditional commercial fiduciaries are not nearly as invested as digital firms in eliciting ongoing personal exposure from, or monetizing the personal data of, their customers.[45] The potential conflicts between equity owners and end users that arise from these practices are not isolated or incidental but cut to the core of the firms' business.

Traditional fiduciaries are also embedded in thicker relationships of care. Doctors, lawyers, and accountants have a limited number of clients or patients on whose behalf they perform specialized tasks and exercise judgment, in all cases guided by the beneficiary's individual preferences and circumstances as well as by shared norms of a knowledge community.[46] Within the context of such relationships, the law is generally able to manage the problem of divided loyalties by requiring fiduciaries to minimize self-dealing and obvious conflicts; to furnish informed disclosure when conflicts are unavoidable; and, above all, to prioritize the interests of clients and patients over the fiduciary's own interests and the interests of any other beneficiaries.[47]

Would the same legal strategies work for digital information fiduciaries? Can the duties they already owe to stockholders be harmonized with the new duties they would owe to users without doing too much violence either to the companies themselves or to fundamental principles of fiduciary law?

II. FIDUCIARIES IN WHAT SENSE?

A. Managing Divided Loyalties

Balkin has never squarely addressed the issue of cross-cutting loyalties.[48] Nor, as far as we can tell, has any other advocate of the information-fiduciary proposal. But it is possible to imagine at least four ways one might try to reconcile a corporation like Facebook's fiduciary obligations to stockholders with fiduciary obligations to users.

---

[45] Balkin, *Three Laws of Robotics*, *supra* note 7, at 1229; *see also* Balkin, *Triangle*, *supra* note 5, at 2049 (contrasting social media companies and search engines, on the one hand, with doctors and lawyers, on the other, and remarking that the former "will always be tempted to use the data [they collect] in ways that sacrifice the interests of their end users to the company's economic or political interests").

[46] On the idea of professions as knowledge communities, see Claudia E. Haupt, *Professional Speech*, 125 YALE L.J. 1238, 1241–42, 1248–54 (2016).

[47] *See, e.g.*, MODEL CODE OF PROF'L RESPONSIBILITY EC 5-1 (Am. Bar Ass'n 1980) ("The professional judgment of a lawyer should be exercised . . . solely for the benefit of his client and free of compromising influences and loyalties. Neither his personal interests, the interests of other clients, nor the desires of third persons should be permitted to dilute his loyalty to his client."); Robert W. Hillman, *Loyalty in the Firm: A Statement of General Principles on the Duties of Partners Withdrawing from Law Firms*, 55 WASH. & LEE L. REV. 997, 1031 (1998) (observing that across numerous areas of legal practice "the overriding value of protecting the interests of clients serves to temper fiduciary duties that run between law partners"); Martha S. Swartz, *"Conscience Clauses" or "Unconscionable Clauses": Personal Beliefs Versus Professional Responsibilities*, 6 YALE J. HEALTH POL'Y, L. & ETHICS 269, 348 (2006) (noting that the principle that "the 'patient's interest comes first'" "appears in all medical professionals' codes of ethics").

[48] Indeed, the term "Delaware" does not appear once in any of Balkin's writings in this area.

First, it might be argued that Delaware law does not categorically demand that the interests of shareholders (or the corporation itself, understood in some distinct sense[49]) be prioritized over the interests of other constituencies. If this were true, then perhaps a Facebook director's duties to stockholders could simply be subordinated to her duties to users when the two collide, much like a law firm partner's duties to her fellow partners must sometimes give way to her duties to clients. The fundamental flaw in this argument, however, is that it runs counter to the prevailing understanding of Delaware doctrine—which, according to the Chief Justice of the Delaware Supreme Court, "could not have been more clear" since the mid-1980s "that directors of a for-profit corporation must at all times pursue the best interests of the corporation's stockholders."[50]

Second, it might be argued that reforms to advance the best interests of users by reducing addiction, limiting advertising, protecting privacy, and so on would *also* advance the best interests of an online platform and its shareholders, for instance because fostering trust in the present period may make it easier to retain and recruit users in future periods. Delaware law broadly permits, and on some accounts even requires, directors to take a long-run perspective.[51] The fact that corporations like Facebook have persistently declined to self-regulate along such lines,[52] however, suggests that their boards do not see these reforms as likely to enhance firm value or shareholder wealth either in the short or the long term.

Third, as alluded to above,[53] corporate law might be modified through state or federal legislation to authorize or compel platforms to put users' interests ahead of stockholders' interests (either in general or in specific respects). In a much-noted 2016 essay in *The Atlantic*, Balkin and Zittrain call for a preemptive federal statute to strike "a new, grand bargain organized around the idea of fiduciary responsibility."[54] As they describe it, however, the state and local laws this statute would displace are not laws about shareholder primacy but rather "laws about online privacy."[55] At no point has Balkin or Zittrain instructed that their proposal would require modification of companies' existing fiduciary duties to accommodate new duties to users.

---

[49] *See generally* Robert Barlett & Eric Talley, *Law and Corporate Governance*, *in* 1 THE HANDBOOK OF THE ECONOMICS OF CORPORATE GOVERNANCE 177, 194–99 (Benjamin E. Hermalin & Michael S. Weisbach eds., 2017) (discussing the persistent "ambiguity" in Delaware fiduciary law about how to handle situations in which "the interests of the corporation writ large" appear to diverge from "the short-term interests of its common shareholders").

[50] Leo E. Strine, Jr., *The Dangers of Denial: The Need for a Clear-Eyed Understanding of the Power and Accountability Structure Established by the Delaware General Corporation Law*, 50 WAKE FOREST L. REV. 761, 771 (2015).

[51] *See* Odoner, Radin, Goltser & Blumberg, *supra* note 31, at 4.

[52] *See, e.g.*, DIGITAL, CULTURE, MEDIA & SPORT COMM., UK HOUSE OF COMMONS, DISINFORMATION AND 'FAKE NEWS': FINAL REPORT 20–42 (2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf (detailing how Facebook has repeatedly taken actions that increased revenue at the expense of users' privacy and data security).

[53] *See supra* text accompanying note 33.

[54] Balkin & Zittrain, *supra* note 5.

[55] *Id.*

On the contrary, information-fiduciary advocates generally appear to endorse a fourth and final strategy for managing conflicts between stockholders and users, which is to cabin any fiduciary duties afforded to users so that they do not seriously threaten firm value—and thus might even be implemented by judges in the absence of legislation.[56] Balkin has stated repeatedly that the new obligations he would impose on entities like Facebook, Google, and Twitter are "more limited" than the obligations imposed on lawyers, doctors, and accountants.[57] One way to understand this formulation is as an effort to elicit better behavior from digital companies without undermining the shareholder primacy norm. If traditional professional fiduciaries must temper their duties to investors (if there are any) and other beneficiaries with a higher duty of loyalty to patients and clients, it seems that Facebook, Google, and Twitter would, as a rule, have to temper their duties to users with a higher duty of loyalty to shareholders. Delaware law would remain unaffected. The interests of shareholders would still come first.[58]

Pursuant to this strategy, reformers may indeed be able to mitigate the problem of conflicting fiduciary obligations and purchase legal coherence—but at a steep price. For if the concept of digital information fiduciaries does *not* require online platforms to place their users' interests above all other interests, it is unclear what work the concept is supposed to be doing. More than that, it is unclear how this is a fiduciary approach in any meaningful sense.

B. Online Behavioral Advertising and the Implausibility of Putting Users First

Balkin is quick to emphasize that fiduciary duties are not one-size-fits-all in the law and that they can and do vary from context to context.[59] This is true, but within limits. The one thing that does not vary, in contexts where professional firms owe fiduciary duties to individual customers, is that the fiduciary always must act in the customer's best interest. As Zittrain himself has written,

---

[56] It is unclear whether, and how, Balkin believes judges could implement his proposal on their own, without prior statutory or regulatory reform, but certain passages seem to hold out the possibility of a lead role for courts in defining as well as enforcing new fiduciary obligations. *See, e.g.*, Balkin, *Fixing Social Media*, *supra* note 5, at 15 (asserting that one advantage of the fiduciary approach is it "can be implemented . . . by judges, legislatures, or administrative agencies"); Balkin, *Digital Age*, *supra* note 5 (suggesting that "common law courts," as distinct from "the state," might "treat online service providers as information fiduciaries").

[57] *E.g.*, Balkin, *Information Fiduciaries*, *supra* note 5, at 1226; Balkin, *Three Laws of Robotics*, *supra* note 7, at 1229; Balkin, *Fixing Social Media*, *supra* note 5, at 12.

[58] For the reasons given in the main text, this strikes us as the most natural reading of the literature to date. In recent conversations, Balkin has informed us that he assumes the corporate-law fiduciary duties owed by digital platform directors *would* have to be curtailed in important respects to operationalize his proposal. That is, Balkin embraces a version of the third strategy on our list. We will consider this Essay a (partial) success if it pushes Balkin and other advocates of the information-fiduciary idea to clarify their position here—and to grapple explicitly with the question of whether and to what extent they envision sacrificing stockholders' economic interests to advance users' noneconomic interests.

[59] *See, e.g.*, Balkin, *Information Fiduciaries*, *supra* note 5, at 1223 ("[A] changing society generates new kinds of fiduciary relations and fiduciary obligations that the law can and should recognize. The scope of the fiduciary duty, however, is not the same for every entity."); Balkin, *Digital Age*, *supra* note 5 ("[T]here are many types of fiduciary duties.").

"at its core [a fiduciary relationship] means that the professionals are obliged to place their clients' interests ahead of their own."[60]

Abandon this core tenet, and it is unclear what is left of the legal analogy to doctors, lawyers, accountants, and estate managers. The social media executive who is exhorted to treat users well (and prohibited from engaging in certain especially egregious behaviors) yet not required to place users' interests first resembles, instead, the used car dealers and restauranteurs who are classic examples in the case law of service providers who are *not* fiduciaries for their customers.[61] "Although each of these relationships involves significant information asymmetries," as Professor Evan Criddle has explained, "the relationships are all presumptively arm's-length; none by definition involves an entrustment of power from one party to another to be exercised under a purposive and other-regarding mandate."[62] Again, the United States Congress or the Delaware General Assembly could impose a broad user-regarding mandate on social media companies and thereby try to create duties of loyalty and care where none currently exist. But to succeed in this effort and wind up with anything recognizable as a fiduciary relationship, it seems to us that the legislators would have to force fundamental changes in the companies' business practices—changes that information-fiduciary advocates have suggested are unnecessary and unwarranted[63]—and preempt or dilute the stockholder-regarding norms under which the companies currently operate.

Part III will consider the practices that digital information fiduciaries, on Balkin's account, would be barred from engaging in. But Balkin is clear that at least one core practice would survive his reforms: the selling of targeted advertisements tied to personally identifiable information.[64] This concession alone highlights how strained the fiduciary designation is here. A business model built around behavioral advertising[65] demands that companies like Facebook assemble a

---

[60] Zittrain, *Fix This Mess*, *supra* note 5; *see also* Bayer v. Beran, 49 N.Y.S.2d 2, 5 (1944) ("The fiduciary must subordinate his individual and private interests to his duty . . . whenever the two conflict."); John C. Coffee, Jr., *The Mandatory/Enabling Balance in Corporate Law: An Essay on the Judicial Role*, 89 COLUM. L. REV. 1618, 1658 (1989) (describing as the "central conceptual difference" between contracting parties and fiduciaries "that a contracting party may seek to advance his own interests in good faith while a fiduciary may not"); Evan J. Criddle & Evan Fox-Decent, *A Fiduciary Theory of Jus Cogens*, 34 YALE J. INT'L L. 331, 350 (2009) ("In all cases the fundamental fiduciary duty is to exercise the entrusted power exclusively for the other-regarding purposes for which it is held or conferred.").

[61] *See* Evan J. Criddle, *Liberty in Loyalty: A Republican Theory of Fiduciary Law*, 95 TEX. L. REV. 993, 1041 (2017).

[62] *Id.* "The injuries that arise within these relationships can be remedied," accordingly, through nonfiduciary regimes "such as contract law, tort law, property law, and criminal law." *Id.*

[63] *See supra* notes 19–24, 54–58 and accompanying text.

[64] *See, e.g.*, Balkin, *Information Fiduciaries*, *supra* note 5, at 1227 ("It cannot be the case that the basic business model of free or subsidized online services inherently violates fiduciary obligations . . . ."); Balkin, *Fixing Social Media*, *supra* note 5, at 12 ("Social media companies and search engines provide free services in exchange for the right to collect and analyze personal data and serve targeted ads. This by itself does not violate fiduciary obligations.").

[65] The Federal Trade Commission has defined online behavioral advertising as the practice, "typically invisible to consumers," of "tracking . . . consumers' online activities in order to deliver tailored advertising" that is more closely aligned with their "inferred interests." FED. TRADE COMM'N, FTC STAFF

maximally detailed portrait of their users' lives, which the companies then sell to marketers and developers.[66] While targeted advertising is not new, the internet has vastly expanded its scope and sophistication. Advertising of this sort may have some benefits.[67] Balkin asserts that it "allows more efficient advertising campaigns" and can "give social media [companies] opportunities to structure and curate content for end users that they will find most engaging and interesting."[68] Yet as long as such companies make most of their money through personally targeted advertisements, they will be economically motivated to extract as much data from their users as they can—a motivation that runs headfirst into users' privacy interests as well as any interests users might have in exercising behavioral autonomy or ensuring that their personal data is not stolen, sold, mined, or otherwise monetized down the line.[69]

REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 2 (2009), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf.

[66] Facebook denies that it sells user data to third parties. But as Professor Michal Kosinski has pointed out, any time a user clicks on an advertisement, Facebook automatically reveals facets of the user's identity to the advertiser by virtue of the fact that the advertiser has paid Facebook to target specific types of individuals. Michal Kosinski, *Congress May Have Fallen for Facebook's Trap, but You Don't Have to*, N.Y. TIMES (Dec. 12, 2018), https://www.nytimes.com/2018/12/12/opinion/facebook-data-privacy-advertising.html. And as Professor Chris Hoofnagle has observed, Facebook also grants access to user data to developers, a form of exchange that he argues should also be considered a "sale." Chris Hoofnagle, *Facebook and Google Are the New Data Brokers*, DIGITAL LIFE INITIATIVE @ CORNELL TECH (Jan. 16, 2019), https://www.dli.tech.cornell.edu/blog/facebook-and-google-are-the-new-data-brokers.

[67] Whether and under what conditions online behavioral advertising actually enhances consumer welfare is debated. *See, e.g.*, Veronica Marotta, Kaifu Zhang & Alessandro Acquisti, Who Benefits from Targeted Advertising? 2–5 (2015) (unpublished manuscript), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00037-100312.pdf (reviewing potential costs and "benefits of increasingly widespread and precise collection and usage of consumer data for the targeting of online ads," and developing a model that suggests consumer welfare is generally higher "when *less* information is exchanged" with advertisers (emphasis added)).

[68] Balkin, *Fixing Social Media*, *supra* note 5, at 2.

[69] Some predict that the GDPR will lead to fundamental changes in the business models of Facebook and other behavioral-advertising-based companies, at least in the European Union. *See, e.g.*, Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 1, 109 (2018) (arguing that the GDPR "may be an end to Facebook and Google as they currently operate"); Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 143 (2017) (stating that the GDPR's ban on tying, or the extension of "terms within a single contractual agreement . . . to include processing of personal data beyond that which is necessary to the purpose of the contract," "takes aim at myriad new digital business models based around data trade"); Henry Farrell & Abraham Newman, *Here's How Europe's Data Privacy Law Could Take Down Facebook*, WASH. POST: MONKEY CAGE (May 25, 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/heres-how-europes-gdpr-may-take-down-facebook ("Privacy activist Max Schrems and his new organization . . . have used the GDPR to launch four major court cases against Facebook and its subsidiaries. If Schrems's interpretation prevails, Facebook's business model will be fundamentally challenged."). It is too early to assess these predictions. But it is worth noting that while Facebook's user growth in Europe initially slowed after the GDPR took effect in May 2018, it has since rebounded—without any evident changes to the company's core business model. *See* Elizabeth Schulze, *Facebook's User Growth in Europe Is Bouncing Back, Defying Stricter Privacy Laws*, CNBC (Apr. 25, 2019), https://www.cnbc.com/2019/04/25/facebook-q1-2019-user-growth-in-europe-is-bouncing-back-despite-

Balkin acknowledges that permitting online providers to collect personal data and serve targeted advertisements "creates a perpetual conflict of interest" between the providers and their users.[70] Rather than see this as an insuperable obstacle to a fiduciary relationship, however, he submits that "the goal should be to ameliorate or forestall conflicts of interest."[71] "[T]he law should limit how social media companies can make money off their end users, just as the law limits how other fiduciaries can make money off their clients and beneficiaries."[72] Sketching out what these limits might look like, Zittrain suggests that a digital information fiduciary would be prohibited from harnessing user data to enable "predatory" advertisements but permitted to expose users to nonpredatory advertisements.[73]

Even if we accept for argument's sake the soundness of the predatory/nonpredatory distinction in this context—although we are doubtful[74]—it is unclear how a digital fiduciary is supposed to fulfill its duty of loyalty to users under conditions of profound and "perpetual" conflict. Fiduciary theorists debate the best way to conceptualize the duty of loyalty. On thicker, "prescriptive" accounts, a loyal fiduciary must not only avoid conflicts of interest but also act with "affirmative devotion" or "obedience" toward her beneficiary.[75] On thinner, "proscriptive" accounts, the fiduciary must "avoid conflicts between pursuit of his self-interest and fulfilment of his duty to act

---

gdpr.html. Facebook is currently the subject of over a dozen GDPR-related investigations, including ten by the Irish Data Protection Commission. *See* Alex Scroxton, *Facebook Facing 10 GDPR Investigations in Ireland*, COMP. WKLY. (Mar. 1, 2019), https://www.computerweekly.com/news/252458664/Facebook-facing-10-GDPR-investigations-in-Ireland.

[70] Balkin, *Fixing Social Media*, *supra* note 5, at 13; *see also* Balkin, *Information Fiduciaries*, *supra* note 5, at 1226 ("The value of end-user data and its centrality in the business models of many online service providers, creates an inherent potential for conflicts of interest between the digital company and the end-user."); Zittrain, *Fix This Mess*, *supra* note 5 ("It may be that aspects of an advertising-based business model are indeed incompatible with ethically serving users . . . .").

[71] Balkin, *Fixing Social Media*, *supra* note 5, at 13.

[72] *Id.*

[73] *See* Zittrain, *How to Exercise*, *supra* note 5 ("A fiduciary duty wouldn't broadly rule out targeted advertising—dog owners would still get dog food ads—but it would preclude predatory advertising, like promotions for payday loans.").

[74] *Cf.* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 90 (2019) ("The word 'targeted' is another euphemism. It evokes notions of precision, efficiency, and competence. Who would guess that targeting conceals a new political equation in which Google's concentrations of computational power brush aside users' decision rights as easily as King Kong might shoo away an ant, all accomplished offstage where no one can see?"); Louise Matsakis, *Facebook's Targeted Ads Are More Complex Than It Lets On*, WIRED (Apr. 25, 2018), https://www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on (noting that "companies who use Facebook have a near-endless number of data points with which to target their ads," allowing them to pick out "hyper-specific audiences with extreme precision," and that users are significantly more likely to click on "psychologically tailored ads"); Piety, *supra* note 31 (arguing that "the vast majority of [online] advertising practices are . . . manipulative in ways that people may not fully appreciate and [that] may encourage anti-social, unhealthy, or self-defeating behaviors or practices").

[75] Paul B. Miller & Andrew S. Gold, *Fiduciary Governance*, 57 WM. & MARY L. REV. 513, 557–59 (2015).

for the benefit of the beneficiary" and "between this duty and the pursuit of others' interests."[76] Even under this *less* demanding theory of loyalty, fiduciary law cannot tolerate an arrangement that places the fiduciary's economic livelihood and its beneficiaries' well-being fundamentally at odds. The whole point of proscriptive rules implementing the duty of loyalty is to minimize "biasing factors that might induce the fiduciary to subjugate the interests of beneficiaries" to any other end.[77]

To appreciate just how odd it is to think that a behavioral-advertising company could be a fiduciary for its users, imagine visiting a doctor—let's call her Marta Zuckerberg—whose main source of income is enabling third parties to market you goods and services. Instead of requesting monetary payment for services rendered, Dr. Zuckerberg floods you (and her two billion other patients) with ads for all manner of pills and procedures from the second you set foot in her office, and she gets paid every time you try to learn more about one of these ads or even look in their direction. In fact, this is just about the only way she gets paid—as her financial backers are apt to remind her. The ads themselves, moreover, are tightly tailored to your economic, demographic, and psychological profile and to any consumer frailties you exhibit.[78] They are also continually updated in light of information Dr. Zuckerberg collects on you; to be sure she does not miss anything, she has planted surveillance devices all around your neighborhood as well as her office.[79] Can this institutional and incentive structure plausibly be reconciled with a commitment to prioritizing your health?[80]

---

[76] *Id.* at 557 (internal quotation marks omitted).

[77] *Id.*

[78] *See generally* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014). Dr. Zuckerberg may even assign scores to patients based on their susceptibility to certain sorts of ads, and then share those scores with third parties. *See generally* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014).

[79] Your data, accordingly, *is* the payment you make to Dr. Zuckerberg. *Cf.* Shoshana Zuboff, *The Real Reason Why Facebook and Google Won't Change*, FAST COMPANY (Feb. 22, 2019), https://www.fastcompany.com/90303274/why-facebook-and-google-wont-change ("Users [of Facebook] are not customers . . . . They are merely free sources of raw material.").

[80] Consider, by way of contrast with this hypothetical, the rules limiting real-life doctors from receiving gifts valued $100 or more from pharmaceutical company sales representatives. *See* Elaine K. Howley, *Do Drug Company Payments to Doctors Influence Which Drugs They Prescribe?*, U.S. NEWS & WORLD REP. (Aug. 31, 2018), https://health.usnews.com/health-care/patient-advice/articles/2018-08-31/do-drug-company-payments-to-doctors-influence-which-drugs-they-prescribe (describing these rules). Of course, Facebook is not a health care provider, and prioritizing a medical patient's interests may require very different activities and assurances than prioritizing a social network user's interests. Our point is simply that unlike doctors, Facebook does not come close to putting its customers first in any serious sense—notwithstanding Zuckerberg's protestations to the contrary, *see, e.g.*, Mark Zuckerberg, *The Facts About Facebook*, WALL ST. J. (Jan. 24, 2019), https://www.wsj.com/articles/the-facts-about-facebook-11548374613—and that this follows from the structure of its business.

Apart from the business model, perhaps the most basic distinction between a real-life doctor and Facebook is that a doctor is a trained professional who makes individualized judgments, whereas Facebook is an automated communications network. We bracket in this Essay the deep questions raised by the notion that a fiduciary's relationship with its beneficiaries could be mediated almost entirely by computer algorithms, although we note that Balkin's theory is potentially vulnerable on this ground as well. As Professor Julie Cohen puts it in a response piece:

In other words, the business model matters. It determines the degree to which a commercial enterprise is motivated to advance the best interests of its customers, or the exact opposite. Although the economic incentives of commercial fiduciaries will sometimes diverge from the interests of their customers and raise difficult issues at the margins—indeed, perfect alignment might obviate the need for fiduciary duties in the first place[81]—there are cases where the degree of misalignment renders fiduciary loyalty implausible. Businesses built on behaviorally targeted advertising appear to be one such case.

Moreover, if Balkin's fiduciary obligations may be too weak or too compromised where they apply, one might also worry that they do not apply widely enough. Balkin never discusses the advertisers or content producers who rely on social media companies such as Facebook. Nor does he discuss the millions of *non*users whose data is systematically swept up by Facebook through user uploads of phone and email contacts[82] and through "sites that use Facebook's advertising pixel or other social APIs linking back to Facebook."[83] Like Facebook's end users, these parties surrender to Facebook certain forms of information that they have an interest in keeping private. Facebook, however, has an economic incentive to monetize this information as well. For example, even though an advertiser is unlikely to want its marketing campaign data to be shared with competitors, Facebook may incorporate this data into its algorithms regardless—thereby passing on to rivals the benefits of the advertiser's proprietary information. Many advertisers and content producers are just as captive to Facebook as its end users are, or even more so. Insofar as the purpose of the information-fiduciary proposal is to rebalance the relationship between dominant online intermediaries and those who depend on them, it is unclear why its protections should cover only one set of dependents.

> Classic fiduciaries—doctors, lawyers, priests—operated on small scales and at human rhythms for a reason. The fiduciary construct implies a mutual encounter predicated on the knowability of human beings as human beings, with mutually intelligible desires and needs. The information fiduciaries proposal abstracts speed, immanence, automaticity, and scale away from that encounter and then assumes they never mattered in the first place.

Julie E. Cohen, *Scaling Trust and Other Fictions*, LAW & POL. ECON. [cite].

[81] *Cf.* Tamar Frankel, *Fiduciary Law*, 71 CALIF. L. REV. 795, 811 (1983) ("When the fiduciary's interests coincide with those of the entrustor, the entrustor is partially protected because as the fiduciary acts in his own interest he will automatically act in the interest of the entrustor. . . . The fiduciary may have an incentive to abuse his power, however, if the loss from the joint enterprise is smaller than his gain from abuse of his power.").

[82] *See* Kashmir Hill, *How Facebook Figures Out Everyone You've Ever Met*, GIZMODO (Nov. 7, 2017), https://gizmodo.com/how-facebook-figures-out-everyone-youve-ever-met-1819822691.

[83] Kurt Wagner, *This Is How Facebook Collects Data on You Even If You Don't Have an Account*, RECODE (Apr. 20, 2018), https://www.recode.net/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg; *see also* David Ingram, *Facebook Fuels Broad Privacy Debate by Tracking Non-Users*, REUTERS (Apr. 15, 2018), https://www.reuters.com/article/us-facebook-privacy-tracking/facebook-fuels-broad-privacy-debate-by-tracking-non-users-idUSKBN1HM0DR ("Facebook often installs cookies on non-users' browsers if they visit sites with Facebook 'like' and 'share' buttons, whether or not a person pushes a button."); Wagner, *supra* ("There is no way to opt out of this kind of data collection.").

C. Constructed Vulnerability

Beyond their reliance on targeted advertising, other practices of certain online platforms strain the fiduciary paradigm. Balkin notes that a basic feature of the expertise-based fiduciary relationships on which he focuses is that the fiduciary stands in a position of power over the beneficiary.[84] The sources of this relational power are typically twofold. First, the fiduciary possesses professional skills and competencies that the beneficiary lacks. This explains both why the beneficiary is seeking the fiduciary's services and why she is hampered in monitoring the fiduciary's conduct. Second, obtaining the fiduciary's services requires the beneficiary to disclose personal information that the fiduciary could potentially abuse.[85] The fiduciary's expertise and the beneficiary's vulnerability are thus interrelated in a deep sense.

Balkin suggests that end users' relationships with online platforms involve a similar combination of (1) valuable expertise and (2) personal exposure necessary to enlist that expertise.[86] Each proposition warrants scrutiny.

Whether an online platform offers expertise may vary. In the case of Facebook, users are offered, first and foremost, access to a communications network, a vast infrastructure for social and economic exchange.[87] Facebook employs hundreds of skilled professionals, such as the software engineers who create and maintain its database applications and search functions. But so do automobile manufacturers, oil and gas outfits, and any number of other firms not traditionally seen as fiduciaries for their customers. Expertise underwrites commercial fiduciary law only insofar as it enables specialized, individualized judgments and services to be rendered on the beneficiary's behalf. Individuated experience on Facebook is largely limited to choosing certain settings and inputting certain information (friends requested, groups joined, posts "liked"), which trigger a series of automated responses. Maintaining a twenty-first-century version of the Yellow Pages coupled with a telecommunications infrastructure and search database requires significant technical expertise, to be sure, but not the kind of expertise that has helped justify fiduciary relationships in the past.

The one Facebook service that has involved a more context-sensitive form of judgment is content moderation. Content moderation refers to the practice of establishing and enforcing a set

---

[84] *See, e.g.*, Balkin, *Information Fiduciaries*, *supra* note 5, at 1216–17.

[85] *See id.*; *see also* Frankel, *supra* note 81, at 810 ("The delegated power that enables the fiduciary to benefit the entrustor also enables him to injure the entrustor, because the purpose for which the fiduciary is allowed to use his delegated power is narrower than the purposes for which he is capable of using that power.").

[86] *See, e.g.*, Balkin, *Information Fiduciaries*, *supra* note 5, at 1222 ("[E]nd-users' relationships with many online service providers involve significant vulnerability, because online service providers have considerable expertise and knowledge and end-users usually do not. Online service providers have lots of information about us, and we have very little information about them . . . .").

[87] *Cf.* K. Sabeel Rahman, *The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept*, 39 CARDOZO L. REV. 1621, 1669 (2018) (describing Facebook, Google, and Amazon as leading "examples of online-enabled infrastructure for the modern economy").

of rules to govern which kinds of speech are permitted on a platform.[88] Facebook's content moderators, however, do not apply their judgment for the benefit of any given user. Rather, they are called upon to protect community standards and the economic viability of the platform as a whole.[89] In this way, an online content moderator is more akin to a traffic cop—applying rules that benefit the collective and help keep traffic flowing—than to a doctor or a lawyer. The fact that Facebook outsources the vast majority of its content moderation jobs,[90] moreover, is some indication that it does not view the service as a core part of the business.[91]

What about exposure? Here, too, the nature of the problem is notably distinct. Unlike in the case of obtaining legal advice or medical care, the sharing of intimate personal information with the provider is not a functional prerequisite to accessing Facebook or any other social media network. It is the price the online providers have chosen to set. Doctors and lawyers need to learn sensitive details about the individuals who engage their services to be able to serve them well. Social media companies do not.

The loss of privacy and control experienced by Facebook users therefore does not stem, organically, "from the structure and nature of the fiduciary relation."[92] It stems from Facebook's deliberate efforts to *create* such vulnerabilities. Facebook's dominant market position supports this strategy. To the extent that users feel beholden to Facebook, it is not because the company offers them especially skillful services or judgments so much as because of a lack of viable alternatives.[93] By virtue of owning four of the top five social media applications, Facebook makes

[88] For an overview and analysis of how platforms like Facebook moderate user-generated content, see Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1630–62 (2018).

[89] *See, e.g.*, *id.* at 1625 ("Platforms create rules and systems to curate speech out of a sense of corporate social responsibility, but also, more importantly, because their economic viability depends on meeting users' speech and community norms.").

[90] *See* Casey Newton, *The Trauma Floor*, VERGE (Feb. 25, 2019), https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona (detailing the psychological trauma that contractors may endure as part of their content moderation jobs, which pay a fraction of what full-time Facebook employees make); Queenie Wong, *Facebook Content Moderation Is an Ugly Business. Here's Who Does It*, CNET (Mar. 1, 2019), https://www.cnet.com/news/facebook-content-moderation-is-an-ugly-business-heres-who-does-it (listing companies that have contracted with Facebook to provide content moderation).

[91] *Cf.* ZUBOFF, *supra* note 74, at 508–09 (discussing the secretive, "outcast function of 'content moderation,'" which always "operates at a distance from the corporation's core functions").

[92] Frankel, *supra* note 81, at 810 (emphasis omitted).

[93] This raises another point of disanalogy with traditional professional fiduciaries: They not only tend to "operate[] on small scales," Cohen, *supra* note 80, but they also generally face meaningful competition. The need to compete with others in their profession gives doctors and lawyers a business reason to serve the interests of their beneficiaries. This is especially true today, when patients and clients can publicly post ratings and reviews. Dominant digital platforms, by contrast, operate in concentrated markets. Whereas the targeted-advertising-based business model of these platforms creates (from a user's perspective) bad incentives, the underlying market structure attenuates good incentives.

it difficult to escape the company's ecosystem.[94] As legal scholars[95] and German antitrust authorities[96] have concluded, this market position enables Facebook to extract more data from its users—who often feel they have nowhere else to go—and thereby compounds their vulnerability.

By glossing over these points of disanalogy with doctors and lawyers, Balkin's proposal risks obscuring the contingent and constructed character of the power imbalances that exist between ordinary individuals and the dominant online providers—imbalances that stem both from the business model these firms employ and from the market dominance they enjoy. This blind spot, in turn, risks foreclosing a broader discussion about interventions that might prevent those imbalances from arising in the first place.

D. First-Order and Second-Order Information Asymmetries

Implicit in the discussion above, traditional fiduciary relationships are marked by asymmetries of information. The duty of loyalty responds to these asymmetries by committing the fiduciary to the beneficiary's best interests and thereby allowing the beneficiary "to take advantage of the [fiduciary's] superior information and expertise" without having "to expend significant resources to monitor the [fiduciary's] behavior."[97] In justifying his proposal, Balkin emphasizes that there are "strong asymmetries of information" between end users and online platforms, whose

[94] In 2017, the top five most popular social media applications were WhatsApp, Facebook, Messenger, Instagram, and Snapchat. Michael Grothaus, *Facebook Owns Four of the Five Most Downloaded Apps in 2017*, FAST COMPANY (Apr. 18, 2017), https://www.fastcompany.com/4035007/facebook-owns-four-of-the-five-most-downloaded-apps-in-2017. Facebook purchased Instagram in 2012 and WhatsApp in 2014. In 2013, Facebook reportedly attempted to purchase Snapchat, but Snapchat rebuffed the offer. *See* John Shinal, *Mark Zuckerberg Couldn't Buy Snapchat Years Ago, and Now He's Close to Destroying the Company*, CNBC (July 14, 2017), https://www.cnbc.com/2017/07/12/how-mark-zuckerberg-has-used-instagram-to-crush-evan-spiegels-snap.html. Users who decided to leave Facebook in light of recent privacy breaches discovered to their dismay that cutting it out entirely would require deleting Instagram and WhatsApp as well. *See* Will Oremus, *If You Delete Facebook, Do You Also Have to Delete Instagram and WhatsApp?*, SLATE (Dec. 22, 2018), https://slate.com/technology/2018/12/can-you-deletefacebook-if-you-dont-also-delete-instagram-and-whatsapp.html; *see also id.* ("After all, the unfortunate reality is that there aren't a lot of prominent social networks that Facebook doesn't own.").

[95] *See* Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 40 (2019) (arguing that Facebook's ability to extract so much data from users "is merely this titan's form of monopoly rents").

[96] *See* Press Release, *Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources*, BUNDESKARTELLAMT (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2 [hereinafter Bundeskartellamt Press Release] (describing a February 2019 decision by the German national competition regulator that "[t]he extent to which Facebook collects, merges[,] and uses data in user accounts constitutes an abuse of a dominant position").

[97] Maxwell J. Mehlman, *Fiduciary Contracting: Limitations on Bargaining Between Patients and Health Care Providers*, 51 U. PITT. L. REV. 365, 390 (1990); *see also* Tamar Frankel, *Fiduciary Duties as Default Rules*, 74 OR. L. REV. 1209, 1244 (1995) ("[I]n fiduciary law, the duty of loyalty is grounded in asymmetric information.").

"operations, algorithms, and collection practices are mostly kept secret" and might be hard to interpret even if they were disclosed.[98] Balkin is surely right about this.

Yet not all information asymmetries are asymmetric in the same way. We might describe the information asymmetries that obtain in traditional fiduciary settings as *second-order* asymmetries: While the beneficiary may not grasp or even hear about any number of technical details concerning the fiduciary's efforts on her behalf, she understands the core terms of their relationship.[99] This shared understanding enables the beneficiary to give meaningful consent and, in many cases, to exercise some control over the fiduciary's behavior.[100] It also identifies the dimension along which the fiduciary is obligated to serve the beneficiary. Because a patient (say) is seeking medical services, the doctor's duty is to protect and promote the patient's health interests.

What happens when the service provider and the customer lack this shared understanding of the core terms of their relationship? We might describe the information asymmetries that obtain in some of the digital settings in question as *first-order* asymmetries: Beyond the technical details of an online platform's operations, algorithms, and data collection practices, the typical user does not even understand—much less approve of—their basic contours. Most Facebook users, to stick with Balkin's main example, rely on the platform to communicate with other Facebook users. According to a recent Pew survey, 74 percent of them do not know that the platform collects data to classify their interests and traits.[101] Other surveys have found that an overwhelming majority of Facebook users do not want to be exposed to *any* targeted political or commercial advertisements, reflecting a "resounding consumer rejection of surveillance-based ads and content."[102] As a rule, it appears that Facebook users tend to be deeply ignorant of the ways the company serves (or disserves) them, and deeply unnerved when they find out.

This is not just an unusually stark asymmetry of information. It is an elaborate system of social control whose terms are more imposed than chosen. Seen in this light, the idea that the law could convert such companies into fiduciaries for their users without the need for fundamental restructuring looks even more far-fetched.

III. SOLVING WHICH PROBLEMS?

If the information-fiduciary proposal would not disrupt the basic business model of online platforms, what would it do to advance users' interests? And how exactly would the new fiduciary

[98] Balkin, *Information Fiduciaries*, *supra* note 5, at 1226.

[99] *Cf.* Dennis F. Thompson, *Democratic Secrecy*, 114 POL. SCI. Q. 181, 185–86, 192–93 (1999) (distinguishing analogously between "first-order" and "second-order" publicity).

[100] *Cf.* David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 271 (2010) ("'Second-order' publicity rules . . . give citizens a platform for participating in the development of 'first-order' secrets, which affords them a degree of comprehension and control.").

[101] Paul Hitlin & Lee Rainie, *Facebook Algorithms and Personal Data*, PEW RESEARCH CTR. (Jan. 16, 2019), http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data.

[102] Joseph Turow & Chris Jay Hoofnagle, *Mark Zuckerberg's Delusion of Consumer Consent*, N.Y. TIMES (Jan. 29, 2019), https://www.nytimes.com/2019/01/29/opinion/zuckerberg-facebook-ads.html.

duties be enforced? Balkin is strikingly unclear on these questions. Reconstructing his potential answers gives still more reason to doubt that a fiduciary characterization is appropriate or that his proposal is adequate to the problems at hand.

A. Substantive Issues

Supporters of the information-fiduciary proposal have touted the "many benefits"[103] and "enormous consequences"[104] its adoption would bring. On closer inspection, however, the main prescriptions that Balkin associates with the proposal turn out not to require fiduciary law or theory at all. Balkin has repeatedly suggested, for instance, that treating digital companies as information fiduciaries will prevent them from acting like "con artists" toward their users.[105] But deception is already prohibited by a suite of state and federal consumer protection statutes,[106] as well as by common law antifraud doctrines and ordinary contract law, which imposes a duty of good faith and fair dealing that (unlike many fiduciary duties) may not be waived or contracted away even in arms-length transactions.[107] When Google was accused in the early 2010s of acting like a con artist by biasing its search results in favor of its own services and passing off content from competing websites as its own, the Federal Trade Commission (FTC) conducted "a wide-ranging

[103] Bloomberg Editorial, *supra* note 9.

[104] Ariel Dobkin, *Information Fiduciaries in Practice: Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 11 (2018).

[105] *See supra* note 20 and accompanying text. "At base," Balkin recently stated, "the obligations of loyalty mean that digital fiduciaries may not act like con artists." Balkin, *Fixing Social Media*, *supra* note 5, at 13.

[106] *See* 15 U.S.C. § 45(a)(1)–(2) (2012) (declaring unlawful all "unfair or deceptive acts or practices in or affecting commerce" and empowering the Federal Trade Commission (FTC) to prevent such acts and practices); Jim Rossi, *Dynamic Incorporation of Federal Law*, 77 OHIO ST. L.J. 457, 463 (2016) ("Many state consumer protection agencies operate under 'mini-FTC Acts' that incorporate [FTC] definitions of 'unfair,' 'deceptive,' or 'misleading' trade practices."); Henry N. Butler & Joshua D. Wright, *Are State Consumer Protection Acts Really Little-FTC Acts?*, 63 FLA. L. REV. 163, 165–66 (2011) (noting that many state mini-FTC Acts are broader than the federal analogue in their definitions of unlawful conduct, the remedies they afford, and their provision of private rights of action); *see also generally* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016) (describing the proactive role of state attorneys general in enforcing privacy norms under state unfair and deceptive trade acts and practices laws); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 543 (2014) (describing the FTC's growing role since the late 1990s in enforcing both privacy statutes and companies' privacy policies).

[107] *See* Paul M. Altman & Srinivas M. Raju, *Delaware Alternative Entities and the Implied Contractual Covenant of Good Faith and Fair Dealing Under Delaware Law*, 60 BUS. LAW. 1469, 1480 (2005) ("The implied covenant of good faith and fair dealing in contract law may not be waived or contracted away by the parties to an agreement."); *see also* Paul MacMahon, *Good Faith and Fair Dealing as an Underenforced Legal Norm*, 99 MINN. L. REV. 2051, 2065 (2015) ("The duty of good faith and fair dealing has been invoked in several thousand [contemporary U.S. contract] cases, often successfully. And the duty has sometimes served as the basis for strikingly liberal impositions of liability."). Standard legal definitions of good faith invoke the "absence of intent to defraud or to seek unconscionable advantage." *Good Faith*, BLACK'S LAW DICTIONARY (10th ed. 2014).

investigation"[108] under the Commission's organic statute that asked, in essence, whether Google had "acted in good faith" toward its users.[109]

At other points, Balkin has suggested that the information-fiduciary model would shelter users from "abusive"[110] and "manipulative"[111] corporate behaviors. But depending on how one defines these terms,[112] almost all such behaviors may likewise be proscribed by state tort law or by state and federal consumer protection statutes, which prohibit "unfair" as well as "deceptive" practices.[113] Perhaps, then, the information-fiduciary model is best understood as a restatement or refinement of consumer protection law, with particular application to online privacy.[114] In that case, however, it is fair to ask why we need an abstract new theorization of the consumer–provider relationship, instead of an institutionally sensitive account of how existing legal norms can be more effectively elaborated and administered, whether by the FTC or a European-style data protection agency.[115]

---

[108] Statement of the Federal Trade Commission Regarding Google's Search Practices at 1, In re Google Inc., FTC File No. 111-0163 (Jan. 3, 2013), https://www.ftc.gov/system/files/documents/public_statements/295971/130103googlesearchstmtofcomm.pdf.

[109] James Grimmelmann, *Speech Engines*, 98 MINN. L. REV. 868, 935 (2014). Professor Grimmelmann argues that the FTC was right to reject the "search bias" allegations against Google, but that the Commission should have given more "thought as to how to carry out" the continual monitoring of Google that it pledged to undertake. *Id.* at 934–36.

[110] *E.g.*, Balkin, *Algorithmic Society*, *supra* note 5, at 1164; Balkin, *Triangle*, *supra* note 5, at 2049; Balkin, *Information Fiduciaries*, *supra* note 5, at 1227–29.

[111] *E.g.*, Balkin, *Triangle*, *supra* note 5, at 2052–53; Balkin, *Information Fiduciaries*, *supra* note 5, at 1227, 1232; Balkin, *Three Laws of Robotics*, *supra* note 7, at 1229.

[112] In his most recent piece on the regulation of social media, Balkin defines manipulation as "techniques of persuasion and influence that (1) prey on another person's emotional vulnerabilities and lack of knowledge (2) to benefit oneself or one's allies and (3) reduce the welfare of the other person." Balkin, *Fixing Social Media*, *supra* note 5, at 4.

[113] *E.g.*, 15 U.S.C. § 45(a)(1) (2012); Cal. Civ. Code § 1770(a) (West 2017).

[114] *Cf.* James Grimmelmann, *When All You Have Is a Fiduciary*, LAW & POL. ECON. [cite] (suggesting that while fiduciary principles are ill-suited to problems of self-dealing, content moderation, and market concentration on online platforms, the "best version" of U.S. information privacy law "would cash out fiduciary principles in specifying when and how platforms can use and share user data").

[115] A number of prominent scholars and advocates have urged the creation of such an agency in the United States, sometimes pointing to the failures of the FTC at protecting the privacy of online platform users. *See, e.g.*, Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 66–68 (1997); *EPIC to Congress: FTC Has Failed to Protect Privacy, New Data Protection Agency Urgently Needed*, ELECTRONIC PRIVACY INFO. CTR. (May 6, 2019), https://epic.org/2019/05/epic-to-congress-ftc-has-faile.html. Other commentators, however, suggest that the FTC may be doing a better job than European data protection agencies at catalyzing and enforcing consumer privacy norms. *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 307–11 (2011). For an overview of the FTC's legal authorities and use of those authorities to regulate privacy and data security, see Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015).

Balkin's frequent refrain that digital information fiduciaries would have to act in "good faith" toward their users[116] is telling in what it leaves out. Again, all parties involved in all contracts, including terms-of-service contracts, must always act in good faith toward each other.[117] As a matter of law, Balkin's proposal would change nothing in this regard. What is distinctive about fiduciaries is that they are generally held to a standard of "*utmost*" good faith.[118] The omission of "utmost" in Balkin's narrative supplies further evidence that he does not really mean to hold online platforms to anything resembling traditional fiduciary obligations, so much as to basic standards of honesty and decency to which they are already held (however imperfect the enforcement).

This is not to say that every prescription Balkin associates with the information-fiduciary model would duplicate existing consumer protection or contract law. In particular, he has suggested in recent writing that digital information fiduciaries would be obligated to vet third parties before affording them access to user data[119] (although not necessarily obligated to obtain users' consent) and prohibited from encouraging addiction among users.[120] If adopted, both suggestions might entail extra legal responsibilities for social media companies. Yet it is precisely in these areas where Balkin's proposal seems to depart from current law that the tensions become most acute between the fiduciary duties he would create and the fiduciary duties that directors owe to shareholders—as a social media company's bottom line certainly *may* benefit from broad data sharing practices and addictive user behaviors. To break new legal ground here, reformers may have to sacrifice shareholder value to a degree that the information-fiduciary literature has not yet acknowledged or considered.

B. Enforcement Issues

If Balkin is vague on the substantive legal duties that digital information fiduciaries would owe to users, he is all but silent on how these new duties would be enforced. He has been similarly

[116] *E.g.*, Balkin, *Algorithmic Society*, *supra* note 5, at 1161; Balkin, *Triangle*, *supra* note 5, at 2053–55; Balkin, *Three Laws of Robotics*, *supra* note 7, at 1228; Jack Balkin, *Mark Zuckerberg Announces That Facebook Is an Information Fiduciary*, BALKINIZATION (Mar. 21, 2018), https://balkin.blogspot.com/2018/03/mark-zuckerberg-announces-that-facebook.html.

[117] *See supra* note 107 and accompanying text.

[118] *See* Robert W. Hillman, *Private Ordering Within Partnerships*, 41 U. MIAMI L. REV. 425, 458 (1987) ("[A]dmonitions concerning the duty of 'utmost good faith' dominat[e] judicial analyses of fiduciary responsibilities." (internal citation omitted)); David E. Pozen, *Constitutional Bad Faith*, 129 HARV. L. REV. 885, 890 (2016) ("Fiduciaries of all sorts are held to a standard of 'utmost good faith.'").

[119] *See, e.g.*, Balkin, *Second Gilded Age*, *supra* note 27, at 1008 ("The duties of care and confidentiality require information fiduciaries to keep data secure and not to disclose it to third parties unless those third parties are equally trustworthy and agree to the same duties of care, confidentiality, and loyalty as the fiduciary."); *see also* Dobkin, *supra* note 104, at 36–43 (proposing similarly that information-fiduciary duties should prohibit sharing data with third parties under certain circumstances); Theodore Rostow, Note, *What Happens When an Acquaintance Buys Your Data? A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REG. 667, 700 (2017) (noting that under Balkin's framework "[t]he responsibilities of information fiduciaries could be expanded to limit what data companies can sell to brokers").

[120] *See, e.g.*, Balkin, *Fixing Social Media*, *supra* note 5, at 14 ("[I]f social media companies are information fiduciaries, they should also have a duty not to use end-user data to addict end users . . . .").

silent on what the remedies for breach would be. These are no small matters given the number of beneficiaries potentially involved, not to mention the many respects in which rights, remedies, and their enforcement are "inextricably intertwined."[121]

In fiduciary law generally, beneficiaries may enforce their rights in court[122] and remedies "tend to be supracompensatory in order to deter abuse."[123] Judges in Delaware and beyond are often loath to "wield the stick" and impose legal liability,[124] but across every private law context of which we are aware, the fiduciary relationship is a juridical relationship overseen by courts. Would the same hold true for the fiduciary relationship between online platforms and their end users? Or would some sort of purely internal or administrative complaint process suffice?

If private judicial enforcement is contemplated, the scale of such litigation could be staggering. As of 2018, Facebook and Google each had well over 200 million users in the United States alone.[125] Given that cases involving newly minted information-fiduciary duties would likely raise a host of novel legal issues and technical complexities, Balkin's proposal has the potential to swallow judicial dockets even with the aid of class actions, all while further undermining the defendant companies' ability to serve their shareholder beneficiaries.

If, on the other hand, private judicial enforcement is not contemplated, then we have to ask once again whether this is an adaptation or an abdication of core fiduciary principles. Notably, the Balkin-inspired legislation introduced by Democratic Senators in December 2018 would treat fiduciary breaches as actionable only by the FTC and, in the FTC's absence, state attorneys general.[126] Short of direct judicial enforcement, it is also available to Balkin to urge courts to enlist fiduciary principles in an indirect, "gap-filling" manner when adjudicating contractual, tort, or statutory claims brought against online platforms. Courts already do a version of this in other contexts.[127] Yet while limiting information-fiduciary duties to indirect enforcement might halt the

---

[121] Daryl J. Levinson, *Rights Essentialism and Remedial Equilibration*, 99 COLUM. L. REV. 857, 858 (1999).

[122] *See, e.g.*, Seth Davis, *The False Promise of Fiduciary Government*, 89 NOTRE DAME L. REV. 1145, 1146 (2014) ("Private law labels some relationships of power and dependence between persons 'fiduciary.' With the label come duties, enforceable through private rights of action . . . .").

[123] Ethan J. Leib, David L. Ponet & Michael Serota, *A Fiduciary Theory of Judging*, 101 CALIF. L. REV. 699, 708 (2013).

[124] Ethan J. Leib, David L. Ponet & Michael Serota, *Translating Fiduciary Principles into Public Law*, 126 HARV. L. REV. F. 91, 101 (2013) ("Within the fiduciary field, courts are long on rhetoric precisely because they rarely wield the stick . . . .").

[125] *See Google—Statistics & Facts*, STATISTA, https://www.statista.com/topics/1001/google (last visited Feb. 18, 2019); *Number of Facebook Users by Age in the U.S. as of January 2018 (in Millions)*, STATISTA, https://www.statista.com/statistics/398136/us-facebook-user-age-groups (last visited Feb. 18, 2019).

[126] Data Care Act of 2018, § 4, S. 3744, 115th Cong. (2018).

[127] *Cf.* John C. Coffee, Jr., *Privatization and Corporate Governance: The Lessons from Securities Market Failure*, 25 J. CORP. L. 1, 28 (1999) (arguing that "the common law's concept of fiduciary duty both enables and instructs the common law judge to fill in the gaps in an incomplete contract"); Jonathan R. Macey, *An Economic Analysis of the Various Rationales for Making Shareholders the Exclusive Beneficiaries of Corporate Fiduciary Duties*, 21 STETSON L. REV. 23, 25 (similar); Pozen, *supra* note 118,

flood of lawsuits, it would relegate these duties to a supporting and possibly marginal legal role, rather than the starring role that advocates seem to have in mind, as well as to a kind of second-class status within the fiduciary family.

The prospect of judicial enforcement also raises questions about how individual users or institutional bodies are supposed to know when an online platform has violated its fiduciary obligations. In recent years, most of the leading examples of data breaches, privacy invasions, and other reckless behaviors by social media companies have been uncovered by journalists, with some of the reporting coming close to two years after the relevant events took place.[128] Robust and enterprising investigative journalism, it seems, would be crucial to identifying fiduciary violations by the dominant online platforms. And yet, the stranglehold that these same platforms have on the digital advertising market is itself one of the biggest threats to the economic viability of such reporting.[129] Whether or not any new fiduciary duties are needed, achieving effective legal enforcement under these conditions may require not just lawsuits but regular investigations and inspections along with the imposition of affirmative duties to disclose data breaches and other compliance failures promptly and publicly.[130]

---

at 890 (noting that principles of good faith may be used by courts "in a 'gap-filling' role to disallow conduct that otherwise would not run afoul of controlling legal texts").

[128] *See, e.g.*, Issie Lapowsky, *The 21 (and Counting) Biggest Facebook Scandals of 2018*, WIRED (Dec. 20, 2018), https://www.wired.com/story/facebook-scandals-2018; Emily Stewart, *Facebook's Very Bad Year, Explained*, VOX (Dec. 21, 2018), https://www.vox.com/technology/2018/12/21/18149099/delete-facebook-scandals-2018-cambridge-analytica; Selina Wang, *Twitter Sold Data Access to Cambridge Analytica-Linked Researcher*, BLOOMBERG (Apr. 30, 2018), https://www.bloomberg.com/news/articles/2018-04-29/twitter-sold-cambridge-analytica-researcher-public-data-access. As far as we are aware, the only significant recent revelation about Facebook not brought to light by journalists occurred when a UK Parliamentarian pressured an app maker engaged in litigation against Facebook into turning over a cache of internal Facebook documents about data and privacy controls. *See* Cyrus Farivar, *Six4Three Exec "Panicked" in UK MP's Office, Gave Up Facebook Internal Files*, ARS TECHNICA (Nov. 26, 2018), https://arstechnica.com/tech-policy/2018/11/six4three-exec-panicked-in-uk-mps-office-gave-up-facebook-internal-files.

[129] *See generally* ZUBOFF, *supra* note 74, at 506–07; Bell & Owen, *supra* note 37; Daniel Funke, *What's Behind the Recent Media Bloodbath? The Dominance of Google and Facebook*, POYNTER (June 14, 2017), https://www.poynter.org/business-work/2017/whats-behind-the-recent-media-bloodbath-the-dominance-of-google-and-facebook. From 2008 to 2017, newsroom employment in the United States dropped by 23 percent, while newspaper employment dropped by nearly double as much. *See* Elizabeth Grieco, *Newsroom Employment Dropped Nearly a Quarter in Less Than 10 Years, with Greatest Decline at Newspapers*, PEW RESEARCH CTR. (July 30, 2018), http://www.pewresearch.org/fact-tank/2018/07/30/newsroom-employment-dropped-nearly-a-quarter-in-less-than-10-years-with-greatest-decline-at-newspapers. Facebook also impedes investigative journalism more directly through its terms of service, which ban reporters and researchers from using automated collection techniques or temporary research accounts to study the platform. *See* Alex Abdo, *Facebook Is Shaping Public Discourse. We Need to Understand How.*, THE GUARDIAN (Sept. 15, 2018), https://www.theguardian.com/commentisfree/2018/sep/15/facebook-twitter-social-media-public-discourse.

[130] The European Union's major privacy law, the GDPR, requires that covered firms notify the relevant authorities of any data breach within seventy-two hours of having become aware of it. Council Regulation 2016/679, 2016 O.J. (L 119), art. 33.

C. Problems Unaddressed

The plight of journalism raises a more general issue. If it is unclear which problems Balkin's proposal would solve, it seems quite clear that the information-fiduciary model would leave many profound problems untouched. This is not the place to offer a detailed inventory, but beyond the issues of privacy and data security that Balkin foregrounds, the dominant online platforms have been credibly associated with a host of social ills, from facilitating interference in U.S. elections;[131] to serving as a tool for the incitement of genocide in Myanmar;[132] to decreasing users' mental and physical health;[133] to enabling discrimination and harassment against women and racial minorities;[134] to amplifying the influence of "fake news," conspiracy theories, and propaganda robots[135] as well as inflammatory and divisive content more broadly.[136] Betrayal of users' trust as to how their data will be handled is just one category of concerns raised by these companies, and not necessarily the most worrisome category.

Many of the broader harms associated with these platforms are magnified or made possible by a behavioral-advertising-based business model coupled with dominant market positions. While these are distinct features—a company could have the business model without the market position, and vice versa—the problems they create tend to be mutually reinforcing. For example, in recent years Google and Facebook together have captured roughly three-quarters of all digital advertising

---

[131] *See, e.g.*, Nancy Scola, *Massive Twitter Data Release Sheds Light on Russia's Trump Strategy*, POLITICO (Oct. 17, 2018), https://www.politico.com/story/2018/10/17/twitter-foreign-influence-operations-910005 ("Twitter and Facebook have been widely criticized since the 2016 election for not doing more to stem the abuse of their platforms by Russians and other foreign actors hoping to manipulate the American political landscape.").

[132] *See, e.g.*, Paul Mozur, *A Genocide Incited on Facebook, With Posts from Myanmar's Military*, N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html (describing "a systematic campaign on Facebook" by members of the Myanmar military to incite violence against the country's Rohingya minority group).

[133] *See, e.g.*, Holly B. Shakya & Nicholas A. Christakis, *A New, More Rigorous Study Confirms: The More You Use Facebook, the Worse You Feel*, HARV. BUS. REV. (Apr. 10, 2017), https://hbr.org/2017/04/a-new-more-rigorous-study-confirms-the-more-you-use-facebook-the-worse-you-feel ("[M]ost measures of Facebook use in one year predicted a decrease in mental health in a later year. We found consistently that both liking others' content and clicking links significantly predicted a subsequent reduction in self-reported physical health, mental health, and life satisfaction."). *See generally* ZUBOFF, *supra* note 74, at 461–65 (reviewing a "growing body of evidence [that] testifies to the psychic toll of life in the hive" of social media, especially for younger users).

[134] *See, e.g.*, Olivier Sylvain, *Discriminatory Designs on User Data*, KNIGHT FIRST AMEND. INST. 3, 8–16 (2018), https://knightcolumbia.org/sites/default/files/content/Sylvain_Emerging_Threats.pdf (discussing such discrimination and harassment and linking them to design features of online intermediaries).

[135] *See, e.g.*, Tim Wu, *Is the First Amendment Obsolete?*, KNIGHT FIRST AMEND. INST. 11–17 (2017), https://knightcolumbia.org/sites/default/files/content/Emerging%20Threats%20Tim%20Wu%20Is%20the%20First%20Amendment%20Obsolete.pdf (discussing the proliferation of "fake news," "junk news," "abusive online mobs," "reverse censorship," and "bots" on leading digital platforms).

[136] *See supra* note 37 and accompanying text.

sales in the United States and an even higher percentage of growth.[137] Their control over digital advertising networks appears to be an important factor behind the past decade's consolidation within the publishing industry and tens of thousands of layoffs at newspapers and magazines.[138] As the professional media has shrunk, more and more local communities have been left with little to no meaningful news coverage.[139] On multiple interacting levels that transcend any given user's experience, the behaviors of a few platforms have been affecting the fabric and functioning of our democracy—often for the worse.

Against this backdrop of platform dominance and democratic decay, the user-centric nature of the information-fiduciary proposal should give pause. The relevant inquiry for legal reformers, it seems to us, should not just be how a firm such as Google or Facebook exercises its power over end users, but whether it ought to enjoy that kind of power in the first place. Limiting the dominance of some of these firms may well have salutary effects for consumer privacy, both by facilitating competition on privacy protection and by reducing the likelihood that any single data-security failure will cascade into a much broader harm.[140] More than that, the very effort to think

[137] *See* Alex Heath, *Facebook and Google Completely Dominate the Digital Ad Industry*, BUS. INSIDER (Apr. 26, 2017), https://www.businessinsider.com/facebook-and-google-dominate-ad-industry-with-a-combined-99-of-growth-2017-4.

[138] Commentary on this subject is copious. In addition to the sources cited *supra* note 129, see, for example, Josh Constine, *How Facebook Stole the News Business*, TECHCRUNCH (Feb. 3, 2018), https://techcrunch.com/2018/02/03/facebooks-siren-call; Roy Greenslade, *Why Facebook Is Public Enemy Number One for Newspapers, and Journalism*, THE GUARDIAN (Sept. 20, 2016), https://www.theguardian.com/media/greenslade/2016/sep/20/why-facebook-is-public-enemy-number-one-for-newspapers-and-journalism; and Michael Miller, *Google Is Not Journalism's Friend and Now It's Trying to Undermine Paywalls*, FIN. REV. (May 31, 2017), https://www.afr.com/opinion/google-is-not-journalisms-friend-and-now-its-trying-to-undermine-paywalls-20170530-gwghgp. In Farhard Manjoo's pithy formulation, "[t]he cause of each [media] company's troubles may be distinct, but collectively the blood bath points to the same underlying market pathology: the inability of the digital advertising business to make much meaningful room for anyone but monopolistic tech giants." Farhad Manjoo, *Why the Latest Layoffs Are Devastating to Democracy*, N.Y. TIMES (Jan. 30, 2019), https://www.nytimes.com/2019/01/30/opinion/buzzfeed-layoffs.html.

[139] *See, e.g.*, Yemile Bucay, Vittoria Elliott, Jennie Kamin & Andrea Park, *America's Growing News Deserts*, COLUM. JOURNALISM REV. (Spring 2017), https://www.cjr.org/local_news/american-news-deserts-donuts-local.php; Riley Griffin, *Local News Is Dying, and It's Taking Small Town America with It*, BLOOMBERG (Sept. 5, 2018), https://www.bloomberg.com/news/articles/2018-09-05/local-news-is-dying-and-it-s-taking-small-town-america-with-it.

[140] For example, one of the biggest data breaches that Facebook suffered over the past year derived from the site serving as a central "passport" to the internet, such that one's Facebook login can serve as a credential for numerous third-party sales. Once hackers stole the single access key, they won access to users' non-Facebook logins as well. *See* Issie Lapowky, *The Facebook Hack Exposed an Internet-Wide Failure*, WIRED (Oct. 2, 2018), https://www.wired.com/story/facebook-hack-single-sign-on-data-exposed. The primary problem here was not necessarily insufficient protection on Facebook's part, so much as the structurally central role that the company plays in the digital realm. On the general relationship between market structure and the capacity to absorb unexpected shocks, see BARRY C. LYNN, CORNERED: THE NEW MONOPOLY CAPITALISM AND THE ECONOMICS OF DESTRUCTION 78–83 (2010); and Peter C. Carstensen & Robert H. Lande, *The Merger Incipiency Doctrine and the Importance of "Redundant" Competition*, 2018 WIS. L. REV. 783.

through the ramifications of platform dominance would force policymakers to grapple with a wide range of systemic concerns that fall outside the fiduciary frame.

To be clear, we do not believe that addressing the dominance of companies like Facebook will remedy the full panoply of harms associated with them. Nor do we view antitrust enforcement as the sole tool for addressing this dominance. Our point here (which we will develop further in section IV.B) is that any broad regulatory framework or "grand bargain"[141] for social media that focuses on abusive data practices, without attending to issues of market structure or political-economic power, is bound to be at best highly incomplete and at worst an impediment to necessary reforms.

IV. WITH WHAT BENEFITS AND COSTS?

We have argued that the information-fiduciary proposal could cure at most a small fraction of the problems associated with online platforms—and to the extent it does, only by undercutting directors' duties to shareholders, undermining foundational principles of fiduciary law, or both. Why, then, has the idea proven so popular?

At a theoretical level, Balkin's proposal is consilient as well as creative; it seems to resolve a tangle of thorny issues with a single, timeworn legal concept. The failure to specify institutional or operational details can thus be held out as a feature, not a bug.[142] At a political level, the proposal comes across as consumer-protective yet conflict-suppressive; it promises to deliver broad social benefits without overly threatening the tech giants or their profits. At an aesthetic level, there is something attractive about the way in which a fiduciary framework would hold platforms to their own rhetoric of trustworthiness. In other areas of law, too, a number of legal scholars have been pressing in recent years for increasingly expansive accounts of fiduciary obligation.[143] Perhaps the very idea of recasting powerful institutions as duty-bound, other-regarding agents, as if they "operate outside the capitalist free-for-all of exchange relations,"[144] has become more alluring in an age of widespread anxiety about the state of capitalism and liberal democracy.

---

[141] Balkin & Zittrain, *supra* note 5; *see supra* notes 54–55 and accompanying text.

[142] *See, e.g.*, Balkin, *Fixing Social Media*, *supra* note 5, at 15 ("The fiduciary approach has many advantages. It is not tied to any particular technology. It can adapt to technological change. It can be implemented at the state or the federal level, and by judges, legislatures, or administrative agencies.").

[143] *See* Grimmelmann, *supra* note 109, at 904 ("[W]e are undergoing something of an academic fiduciary renaissance, with scholars arguing for treating legislators, judges, jurors, and even friends as fiduciaries." (internal citations omitted)); Daniel Yeager, *Fiduciary-isms: A Study of Academic Influence on the Expansion of the Law*, 65 DRAKE L. REV. 179, 184 (2017) (describing "how academic writing, deploying a sense of *fiduciary* so open as to be empty, has influenced courts to designate" an ever-expanding set of actors as fiduciaries); Evan J. Criddle & Evan Fox-Decent, *Keeping the Promise of Public Fiduciary Theory: A Reply to Leib and Galoob*, 126 YALE L.J. F. 192, 193 (2016) (discussing the recent "revival of public fiduciary theory").

[144] Yeager, *supra* note 143, at 183 ("Fiduciaries are said to operate outside the capitalist free-for-all of exchange relations . . . .").

Whatever the sources of its appeal (and there may be different sources for different audiences), the biggest *legal* benefit of Balkin's proposal, on his telling, is that a fiduciary framework would allow regulations enacted in its name to withstand First Amendment challenges that might otherwise be fatal.[145] Meanwhile, Balkin has clarified that his proposal is not meant to be a cure-all and could be complemented with other reforms, including "pro-competition rules or increased antitrust enforcement."[146] The implication is that there is no basis for worrying that the proposal does not accomplish enough on its own.

Both of these arguments are tantalizing. But both, in our view, are seriously flawed. We see little constitutional upside to the information-fiduciary proposal and significant policy downside. Let us consider each issue in turn.

A. The False Promise of First Amendment Flexibility

The First Amendment, Balkin observes, "may be a potential obstacle to laws that try to regulate private infrastructure owners in order to protect end-users[]."[147] For example, broadband companies have challenged network neutrality regulations (unsuccessfully to date) as a violation of their free speech rights.[148] And social media companies might challenge new measures "restricting how they use, distribute, or sell the consumer data that they collect" on the ground that this data is their "speech or knowledge."[149] First Amendment law, at least in its current "Lochnerian" form,[150] works almost exclusively to the advantage of the online platforms. "Instead of empowering users to challenge their policies, the First Amendment empowers the companies themselves to challenge statutes and regulations intended to promote antidiscrimination norms or users' speech and privacy, among other values."[151]

If these companies were to be recognized as fiduciaries for their users, however, Balkin argues that the constitutional calculus would tip in the regulator's favor. He maintains that because the speech that occurs in fiduciary settings concerns special services rendered in the context of special relationships of vulnerability and dependency, the "First Amendment treats information practices

[145] This is a central theme of Balkin's first, and still most extensive, academic statement of the proposal. *See* Balkin, *Information Fiduciaries*, *supra* note 5, at 1209–20.

[146] Balkin, *Fixing Social Media*, *supra* note 5, at 15.

[147] Balkin, *Second Gilded Age*, *supra* note 27, at 982.

[148] *See, e.g.*, U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 740–44 (D.C. Cir. 2016) (rejecting a First Amendment challenge to a 2015 Federal Communications Commission (FCC) order imposing "common carrier" obligations on telecommunications companies). *But cf. id.* at 418 (Kavanaugh, J., dissenting from denial of rehearing en banc) (arguing that the FCC order is unconstitutional because "the First Amendment bars the Government from restricting the editorial discretion of Internet service providers, absent a showing that an Internet service provider possesses market power in a relevant geographic market").

[149] Balkin, *Second Gilded Age*, *supra* note 27, at 982–83.

[150] *See* Jeremy K. Kessler & David E. Pozen, *The Search for an Egalitarian First Amendment*, 118 COLUM. L. REV. 1953, 1959–64 (2018) (reviewing the contemporary debate over "First Amendment Lochnerism"). Roughly speaking, First Amendment Lochnerism refers to "a First Amendment jurisprudence that disables redistributive regulation and exacerbates socioeconomic inequality." *Id.* at 2007.

[151] *Id.* at 1973.

by fiduciaries very differently than it treats information practices involving relative strangers."[152] "Generally speaking, when the law prevents a fiduciary from disclosing or selling information about a client—or using information to a client's disadvantage—this does not violate the First Amendment, even though the activity would be protected if there were no fiduciary relationship."[153] In support of this claim, Balkin cites four state court cases, three from the 1970s and one from the 1990s, recognizing a doctor's duty not to disclose patient information.[154] He also interprets a 1985 securities law case that was decided by the Supreme Court on statutory grounds, *Lowe v. SEC*,[155] as signaling that "ordinary First Amendment doctrine—including even the ban on prior restraints—would not apply to communications" between professional fiduciaries and their beneficiaries.[156]

Balkin's argument here is elegant and insightful, but it does not appear to track the approach that the Roberts Court would actually employ when evaluating First Amendment claims brought by online platforms that had been designated (by Congress, an administrative agency, or the Court itself) as fiduciaries for their users. This past Term, in *National Institute of Family and Life Advocates v. Becerra*, Justice Thomas's opinion for the Court was emphatic that the Court has never "recognized 'professional speech' as a separate category of speech."[157] Nor did the Court see any "persuasive reason" to reconsider that stance now.[158] There is good reason to think that Justice Thomas overstated this point and that certain narrow categories of professional speech, such as doctors' advice to patients, will continue to be treated differently than other categories of speech (or treated as nonspeech) under the First Amendment, unless the Court wishes to wreak havoc on longstanding regimes of professional licensing, informed consent, and malpractice liability.[159] But at a minimum, *Becerra* signals skepticism about Balkin's broader claim that "the law does not treat speech in professional or other fiduciary relationships as part of public discourse" but instead treats such speech "as part of ordinary social and economic activity that is subject to reasonable regulation."[160]

---

[152] Balkin, *Information Fiduciaries*, *supra* note 5, at 1209.

[153] *Id.* at 1210.

[154] *Id.* at 1210 n.120.

[155] 472 U.S. 181 (1985).

[156] Balkin, *Information Fiduciaries*, *supra* note 5, at 1219. Balkin maintains that "most professional relationships are fiduciary relationships." *Id.* at 1209.

[157] 138 S. Ct. 2361, 2371 (2018); *see also id.* at 2371–72 ("Speech is not unprotected merely because it is uttered by 'professionals.'"). Justice Thomas added that the Court "has been especially reluctant to 'exemp[t] a category of speech from the normal prohibition on content-based restrictions.'" *Id.* at 2372 (quoting United States v. Alvarez, 567 U. S. 709, 722 (2012) (plurality opinion)). In her largely sympathetic 2016 response to Balkin, Bambauer anticipated a version of this rejoinder. *See* Bambauer, *supra* note 8, at 1950 ("[A]ny attempt to harness the power of fiduciary relationships in order to achieve broad privacy policy runs into an unavoidable problem: it violates the cardinal rule of content-neutrality.").

[158] *Becerra*, 138 S. Ct. at 2375.

[159] *See* Claudia E. Haupt, *The Limits of Professional Speech*, 128 YALE L.J.F. 185, 188 (2018) (arguing forcefully that "despite the [*Becerra*] Court's insistence that it has never recognized professional speech as a category," professional speech—when "narrowly defined"—is and should remain "a type of speech doctrinally distinct from others").

[160] Balkin, *Information Fiduciaries*, *supra* note 5, at 1217.

Even if the Court were to affirm some sort of relaxed standard of First Amendment review for regulations of traditional fiduciary–beneficiary communications, it is not at all clear that the Court would apply this standard to the special case of digital information fiduciaries. Justice White's concurring opinion in *Lowe*, which was joined by Chief Justice Rehnquist, suggested that regulations of a profession should be given more lenient First Amendment treatment only when there is a "personal nexus between professional and client" and the professional is "exercising judgment on behalf of [a] particular individual with whose circumstances he is directly acquainted."[161] A "personal nexus" of this sort is arguably lacking altogether in the context of online platforms.[162] Moreover, Balkin's crucial concession that the fiduciary duties owed by online platforms to their users will be "more limited"[163] than the duties of traditional fiduciaries leads naturally to the possibility that the government's regulatory leeway may be more limited as well. Balkin is at pains to emphasize that fiduciary relationships are not one-size-fits-all in the law;[164] why, then, should we assume that First Amendment review of these heterogeneous relationships will always take the same form?

In short, the notion that designating online platforms as fiduciaries would yield a significant First Amendment payoff strikes us as resting on an overly simple (if not nominalist) view of how judges would respond to such a designation, and as contradicted by the Roberts Court's case law. Balkin's argument here, in any event, only extends to regulations that could be characterized as speech regulations—most notably, restrictions on what platforms can do with the consumer data they gather. It is inapplicable to other policy tools that could not plausibly be characterized as speech regulations even by proponents of the "data is speech" view,[165] including most antitrust and pro-competition tools, public certification or safe harbor programs "in which companies opt into various promises (backed by regulatory enforcement) in exchange for" certain legal or reputational benefits,[166] requirements that firms pay people for their data,[167] data portability and interoperability mandates,[168] co-regulation schemes that incentivize businesses to continually

[161] *Lowe*, 472 U.S. at 232 (White, J., concurring in result).

[162] *See supra* sections II.B–C.

[163] *See supra* note 7 and accompanying text.

[164] *See supra* note 59 and accompanying text.

[165] *See generally* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014). For a contrary perspective, see, for example, Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1169 (2005) ("I believe that most privacy regulation that interrupts information flows in the context of an express or implied commercial relationship is neither 'speech' within the current meaning of the First Amendment, nor should it be viewed as such." (internal citations omitted)).

[166] Bambauer, *supra* note 8, at 1952. Information-fiduciary principles might themselves be instituted through a safe harbor program, *see* Balkin & Zittrain, *supra* note 5, but so presumably could other, more concrete legal obligations related to the goals of the program.

[167] *See, e.g.*, *Data Workers of the World, Unite*, THE ECONOMIST (July 7, 2018), https://www.economist.com/the-world-if/2018/07/07/data-workers-of-the-world-unite; Eric A. Posner & E. Glen Weyl, *Want Our Personal Data? Pay for It*, WALL ST. J. (Apr. 20, 2018), https://www.wsj.com/articles/want-our-personal-data-pay-for-it-1524237577.

[168] *See, e.g.*, Bennett Cyphers & Danny O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, ELECTRONIC FRONTIER FOUND. (July 24, 2018), https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-

produce and share compliance information[169] and any number of front-end limits or "taxes" on private data collection.[170] Especially given the extraterritorial reach of the GDPR's personal data protections,[171] these sorts of policy tools may have more bite at this time than the regulations Balkin has in mind.

Furthermore, within the domain where it does apply, we question whether Balkin's argument makes the strongest case for the constitutionality of public-interested platform regulation. Balkin grounds his argument in the special nature of the relationships that digital information fiduciaries, like all other fiduciaries, purportedly have with their beneficiaries. First Amendment theory, however, supplies numerous other possible grounds for justifying regulations meant to enhance platform users' privacy, security, and control of their own data—from arguments that commercial speech and computer algorithms deserve only modest (if any) constitutional protection;[172] to the contention that online service providers should be treated as "public trustees"[173] or "public utilities"[174]; to "systemic" perspectives on free speech that read the First Amendment as permitting or even requiring the government to take affirmative measures "to engineer a fairer, fuller, 'freer' expressive environment for everyone."[175]

We are not suggesting that these theories are without serious problems of their own, much less that the Roberts Court is likely to embrace any of them. But neither is the Court likely to embrace Balkin's approach.[176] And whatever their defects, these other theories at least focus attention on the most constitutionally salient feature of companies like Google and Facebook: not that their end users must be able to trust and depend on them, but that they are extraordinarily powerful actors with the potential to do great harm to (as well as good for) the freedoms of speech, assembly, and the press. Put more sharply, a First Amendment jurisprudence that analogizes the dominant online platforms to doctors and lawyers, while ignoring entirely their status as increasingly essential *platforms* for public communication and the "New Governors" of the public sphere,[177] is not credible. It obscures the real social stakes.

---

monopoly-medicine (recommending that the FTC impose such mandates on Facebook as "part of an antitrust remedy or negotiated settlement").

[169] *See, e.g.*, Dani Rodrik & Charles Sabel, Building a Good Jobs Economy 10 (Apr. 2019) (unpublished manuscript) (on file with authors).

[170] *See* Omri Ben-Shahar, *Data Pollution* 6–7, 33–43 (Univ. of Chi. Pub. Law Working Paper No. 679, 2018), https://ssrn.com/abstract=3191231 (contrasting data "taxes" with "command-and-control" limits).

[171] *See* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EU SHAPES GLOBAL MARKETS THROUGH ITS RULES AND REGULATIONS (forthcoming) (on file with authors) (discussing the GDPR's broad extraterritorial reach and "the extent to which [global companies] are choosing to adopt EU privacy policy as their company standard"); Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65, 98 (2019) (providing an overview of the GDPR and the ways in which it "will influence [privacy] policy worldwide").

[172] *See* Kessler & Pozen, *supra* note 150, at 1988 nn.164–65 (collecting sources to this effect).

[173] Wu, *supra* note 135, at 23.

[174] Rahman, *supra* note 87, at 1668–80.

[175] Kessler & Pozen, *supra* note 150, at 2002.

[176] *See supra* notes 157–164 and accompanying text.

[177] Klonick, *supra* note 88, at 1663.

B. Downside Risks

Against this highly speculative and very possibly nonexistent First Amendment upside, a full analysis of the information-fiduciary proposal also needs to consider its potential downsides. We see several significant ones. As with the critical legal and conceptual points raised in Parts II and III, we have not encountered any discussion of these policy risks in the growing literature on the subject.

First, and most simply, a fiduciary framework paints a false portrait of the digital world. It characterizes Facebook, Google, Twitter, and other online platforms as fundamentally trustworthy actors who put their users' interests first. As we tried to show in Part II, this is not a plausible depiction of what most of these companies—even if chastened in the ways Balkin outlines—are really like. The tension between what it would take to implement a fiduciary duty of loyalty to users, on the one hand, and these companies' economic incentives and duties to shareholders, on the other, is too deep to resolve without fundamental reform. To suggest otherwise is to risk mystification of "surveillance capitalism,"[178] entrenchment of prevailing business models, and legitimation of a wide range of troubling practices, if not also the unraveling of fiduciary law itself.[179]

Second, this false portrait of reality invites policy misfires. To a large extent, it seems that Balkin's prescriptions would simply mirror or marginally refine longstanding consumer protection guarantees and antifraud doctrines,[180] in which case our time and energy may be better spent figuring out how to strengthen enforcement of the existing rules rather than proliferating legal categories.[181] Meanwhile, to the degree that Balkin's prescriptions depart from existing consumer protection law,[182] his theory lacks the resources to justify prioritizing those departures over countless other moves that might be made. The "grand bargain organized around the idea of fiduciary responsibility" that Balkin and Zittrain have put forward,[183] in which a new federal statute would preempt state laws about online privacy, strikes us as an especially bad deal for proponents of online privacy, given the watered-down version of fiduciary responsibility such a

[178] *See generally* ZUBOFF, *supra* note 74; *cf.* Kessler & Pozen, *supra* note 150, at 1971–73 (reviewing the critical literature on "informational capitalism" and "communicative capitalism").

[179] Even if "the law of fiduciary obligation has developed through analogy to contexts in which the obligation conventionally applies," Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879, 879, presumably some analogies would be so strained as to degrade rather than coherently advance this developmental process.

[180] *See supra* notes 103–118 and accompanying text.

[181] For a recent argument that the FTC's ability to protect consumer privacy has been "severely curtailed" by the Commission's lack of general rulemaking authority, its reluctance to target unfair practices as distinct from deceptive practices, and inadequate funding levels, among other factors, see Barrett, *supra* note 20, at 1073–78.

[182] *See supra* notes 119–120 and accompanying text.

[183] Balkin & Zittrain, *supra* note 5; *see supra* notes 54–55 and accompanying text.

statute would codify and the "pioneer[ing]" role that state attorneys general have played in enforcing their own unfair and deceptive trade acts and practices laws.[184]

Third, the information-fiduciary proposal conceives of systemic problems in relational terms. The reason a company like Facebook can and should be regulated in a special way, it tells us, is that Facebook has (or should have) a special relationship of trust and dependency with each of its users. Not only does this argument ignore how Facebook generates dependency,[185] but it also recasts what ought to be questions of the public interest—questions about what kind of social media landscape is good for our democracy—in a narrow quasi-contractarian frame that asks, instead, what Facebook owes any given individual who signs up for its service. This framing implicitly downgrades other accounts of the appropriate bases for government intervention and other models of public regulation, in particular those that conceptualize privacy as a public good[186] or that aim to ward off extreme asymmetries of knowledge and power or "structural stranglehold[s] over digital media."[187] By the same token, the information-fiduciary proposal implicitly acquiesces in the legal decisions that enabled certain online platforms to become so dominant. It takes current market structures as a given.

Recently, Balkin has suggested that a fiduciary approach to regulating online platforms can be combined with more ambitious approaches, in effect giving us the best of both worlds.[188] "The fiduciary approach," Balkin writes, "meshes well with other forms of consumer protection" and, "[i]n particular, does not get in the way of new pro-competition rules or increased antitrust enforcement."[189] These policy tools would potentially "restructure how digital advertising operates" and "break up the larger companies into smaller companies that can compete with each other or create a space for new competitors to emerge."[190] Balkin's interest in such tools resonates

---

[184] Citron, *supra* note 106, at 750, 785, 800, 811.

[185] *See supra* section II.C.

[186] On the ways in which digital privacy can be seen as a public good, see generally Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2015); Ben-Shahar, *supra* note 170, at 10–16; and Zeynep Tufekci, *The Latest Data Privacy Debacle*, N.Y. TIMES (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html.

[187] David Pozen, *Authoritarian Constitutionalism in Facebookland*, BALKINIZATION (Oct. 30, 2018), https://balkin.blogspot.com/2018/10/authoritarian-constitutionalism-in.html.

[188] This suggestion is echoed in Barrett, *supra* note 20, at 1107–12; and Grimmelmann, *supra* note 114.

[189] Balkin, *Fixing Social Media*, *supra* note 5, at 15.

[190] *Id*. at 10–11. Traditional antimonopoly and pro-competition remedies include horizontal and vertical breakups, interoperability and portability regimes, and common carriage requirements. For a taxonomy of "competition catalysts" used by agencies like the FTC and FCC, see Tim Wu, *Antitrust via Rulemaking: Competition Catalysts*, 16. COLO. TECH. L.J. 33, 47–61 (2017). For discussions of how some of these remedies might be applied to digital platforms like Facebook, see TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE 132–33 (2018) ("The simplest way to break the power of Facebook is breaking up Facebook."); Barry Lynn & Matt Stoller, *Facebook Must Be Restructured. The FTC Should Take These Nine Steps Now*, THE GUARDIAN (Mar. 22, 2018), https://www.theguardian.com/commentisfree/2018/mar/22/restructure-facebook-ftc-regulate-9-steps-now (proposing a series of reforms for Facebook, including a spinoff of its advertising network, divestiture of WhatsApp and Instagram, and limits on future acquisitions); and Luigi Zingales & Guy Rolnik, *A Way to Own Your Social-Media Data*, N.Y. TIMES (June 30, 2017),

with and responds to a growing body of neo-Progressive scholarship that urges greater emphasis on "structural" (or "infrastructural") solutions to problems of discrimination and domination online.[191]

While we commend Balkin's turn toward structural analysis of this sort, we are deeply skeptical of the claim that the fiduciary approach "meshes well" with it. On the contrary, we suspect that the fiduciary approach, if pursued with any real vigor, would tend to cannibalize rather than complement pro-competition reforms. This fourth and final downside risk may be the most practically consequential of them all.

When introducing the information-fiduciary proposal, Balkin and Zittrain billed it as a kind of regulatory "third way" that could transcend ordinary political divides and policy tradeoffs. Highlighting the proposal's "bipartisan appeal," Zittrain explained that it "protects consumers and corrects a clear market failure without the need for heavy-handed government intervention."[192] Elsewhere, he suggested that a fiduciary approach might "nudge" companies like Facebook to "do the right thing," "without outright requiring it."[193] The details were fuzzy but the message was clear. A fiduciary approach would promote users' interests without necessarily causing too much trouble for the online platforms or their business models, thereby allowing Balkin and Zittrain to win wide support while sidestepping contentious questions like whether to restructure or break up Facebook, as a number of commentators have called for.[194] The basic selling point of the fiduciary approach was that it would be flexible, light-touch, un-"heavy-handed"—in contrast to *and in lieu of* structural reforms.

Balkin's and Zittrain's early advocacy traded on an insight that remains as valid today as it was then: We can regulate the dominant online platforms as information fiduciaries or we can target their market dominance and business models, but very likely we will not do both. To assume otherwise is to overlook the opportunity costs, path dependencies, and expressive effects inherent in creating a new fiduciary regime. Mark Zuckerberg seems to grasp this. He is presumably attracted to the information-fiduciary proposal not just because of its "thoughtful[ness]"[195] and

https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html (advocating a data-portability regime that would reduce the cost of switching social networks and likely generate greater competition).

[191] *See generally, e.g.*, Lina M. Khan, *The Separation of Platforms and Commerce*, 119 COLUM. L. REV. 973 (2019); Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009 (2013); Rahman, *supra* note 87; K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234 (2018); Gigi Sohn, *A Policy Framework for an Open Internet Ecosystem*, 2 GEO. L. TECH. REV. 335 (2018).

[192] Zittrain, *How to Exercise*, *supra* note 5.

[193] Zittrain, *Fix This Mess*, *supra* note 5.

[194] *See, e.g.*, ROGER MCNAMEE, ZUCKED: WAKING UP TO THE FACEBOOK CATASTROPHE 263 (2019); WU, *supra* note 190, at 132–33; Lynn & Stoller, *supra* note 190; Sarah Miller & David Segal, *Break Up Facebook: Latest Hack Proves It's a Dangerous Data Monopoly That a Fine Won't Fix*, USA TODAY (Oct. 5, 2018), https://www.usatoday.com/story/opinion/2018/10/05/facebook-dangerous-monopoly-divest-instagram-whatsapp-messenger-column/1512215002.

[195] Brandom, *supra* note 9 (quoting Zuckerberg).

"intuitive[ness],"[196] but also because of its political implications. An entity that is designated by the government as a loyal caretaker for the personal data of millions of Americans is not an entity that is likely to be dismantled by that same government. Facebook-as-fiduciary is no longer a public problem to be solved, potentially through radical reform. It is a nexus of sensitive private relationships to be managed, nurtured, and sustained.

V. ALTERNATIVE ANALOGIES

This Essay is an exercise in critique, not prescription. We have interrogated the increasingly popular analogy between online platforms and their end users, on the one hand, and professional fiduciaries and their patients and clients, on the other, and we have found this analogy inapposite on multiple levels. Analogical reasoning can retard rather than advance the cause of legal reform when it elides salient institutional differences or normative considerations.[197] Although we do not elaborate any reform program of our own in this Essay, we will close by noting two analogies that strike us as more felicitous starting points than traditional fiduciary relationships for the project of platform regulation.

First, in the case of Facebook, Google, and other dominant online platforms, we might draw an analogy to "offline" providers of social and economic infrastructure.[198] To the degree that these platforms serve as key channels of communication, commerce, and information flow, they can be recognized as controlling the terms of access to essential services. In the Progressive Era, policymakers feared that concentrated private control over infrastructure would create an intolerable imbalance of power between a small number of firms and the communities, businesses, and individuals dependent on them.[199] Regulatory interventions were therefore focused on directly disciplining this power through a combination of legal tools, including nondiscrimination and common carrier regimes, limits on the lines of business in which firms could engage, interoperability requirements, corporate governance reforms, and public options.[200]

The same regulatory principles deserve close consideration today. To the extent that Facebook and Google have achieved their dominance through anticompetitive means, antitrust lawsuits reversing key acquisitions and penalizing forms of monopoly leveraging might play a

[196] *Zittrain and Zuckerberg*, *supra* note 12 (quoting Zuckerberg).

[197] For a valuable argument to this effect, focused on the analogy that some have drawn between digital media companies and traditional news publishers, see generally Whitney, *supra* note 3.

[198] We have already previewed this analogy. *See supra* notes 87 & 191 and accompanying text.

[199] *See* Rahman, *supra* note 87, 1628–39. Professor Rahman defines infrastructure as "those goods and services which (i) have scale effects in their production or provision . . .; (ii) unlock and enable a wide variety of downstream economic and social activities . . .; and (iii) place users in a position of potential subordination, exploitation, or vulnerability if their access . . . is curtailed in some way." *Id.* at 1643.

[200] *See id.* at 1644–47; *see also* GANESH SITARAMAN & ANNE L. ALSTOTT, THE PUBLIC OPTION: HOW TO EXPAND FREEDOM, INCREASE OPPORTUNITY, AND PROMOTE EQUALITY (forthcoming 2019) (describing and defending "public options" that offer people a choice between governmental and private provision of a good or service); Khan, *supra* note 191, at 1037–52 (providing an overview of "separations regimes" applied throughout the twentieth century to proscribe certain organizational structures for railroads, bank holding companies, television networks, and telecommunication carriers).

complementary role, by opening up both primary and adjacent markets.[201] Importantly, however, "structural" interventions do not necessarily have to break up firms. They can also reshape business incentives through bright-line prohibitions on specific modes of earning revenue, and they can reshape markets by creating the conditions for greater competition and consumer autonomy.[202] Data interoperability requirements, for example, allow users to move their data across platforms, which in turn requires incumbent services to continuously compete.[203] A platform that perennially violated users' privacy would not benefit as much from the switching costs that keep users trapped within even unhealthy environments.[204]

Second, in thinking about the regulatory challenges posed by digital platforms' collection, aggregation, and use of personal data, we might draw an analogy to environmental pollution. Professor Omri Ben-Shahar has recently proposed this analogy as a way to move beyond the privacy paradigm in addressing the *social* harms of these practices—not just the concerns they may raise for any given individual subject to surveillance but also the negative externalities they may cause for third parties and for public interests more generally.[205] A pollution perspective helps to highlight why private law solutions are inadequate to the nature of the threat.[206]

The pollution analogy thus points away from individualistic, consumer-centric frameworks and toward a different set of techniques for reducing surveillance-related harms: namely, ex ante prohibitions on which sorts of data can be gathered and to what extent, Pigouvian taxes on data collection and retention that force firms to internalize their social costs, and ex post liability rules for data "spills" and other data disasters that facilitate deterrence and compensation.[207] We take no stance here as to the optimal design of or balance among these techniques. We do, however, endorse the implicit insight that the harms from digital surveillance must be met with clear

[201] Versions of this argument are made by the sources collected in note 194 *supra*.

[202] *See generally* K. SABEEL RAHMAN, DEMOCRACY AGAINST DOMINATION 118 (2016) (distinguishing "structuralist" regulatory strategies, which "limit the underlying powers and capacities" of certain firms, from "prophylactic rules" that rely on "fine-tuning expert management"); Wu, *supra* note 190, at 34 (cataloging a range of "industry-specific statutes, rulemakings, or other tools of the regulatory state to achieve the traditional competition goals associated with the antitrust laws").

[203] Interoperability is thus what Professor Tim Wu calls a "switching cost reducer." Wu, *supra* note 190, at, 35, 56–58; *see also id.* at 56–57 ("Switching costs are a barrier to competition because they require that a competitor not just be slightly better, but quite a bit better to compensate for the costs incurred in changing providers.").

[204] *Cf. supra* notes 92–96 and accompanying text (suggesting that Facebook currently benefits from high switching costs of this sort).

[205] *See generally* Ben-Shahar, *supra* note 170. Other scholars have drawn similar environmental analogies. *See, e.g.*, A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713; Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1 (2006); Ian Samuel, *The New Writs of Assistance*, 86 FORDHAM L. REV. 2873, 2914–24 (2018).

[206] *See* Ben-Shahar, *supra* note 170, at 16–31. Like all analogies, this one is imperfect even if illuminating. *See, e.g.*, Ronen Avraham, *Personal Data as an Environmental Hazard*, JOTWELL (Nov. 14, 2018), https://torts.jotwell.com/personal-data-as-an-environmental-hazard (noting that unlike air pollution, "data pollution does not only create negative externalities, it also creates positive externalities").

[207] *See* Ben-Shahar, *supra* note 170, at 6–7.

prohibitions and economic disincentives, rather than morally laden standards. A fiduciary approach that targets "con artistry"[208] invites the dominant platforms to shun a small set of behaviors and then claim the mantle of trustworthiness, both narrowing the scope of public debate and normalizing the basic operations of surveillance capitalism. By contrast, outright limits or harsh penalties on certain forms of data collection or retention could help to detoxify the larger online ecosystem while preventing platforms from conditioning access to essential services on the ever-greater surrendering of personal data. The German competition authority recently provided an example of such an approach when it ruled that Facebook "will no longer be allowed to force its users to agree to the practically unrestricted collection and assigning of *non*-Facebook data [culled from third-party sources] to their Facebook user accounts."[209] The upshot, the Bundeskartellamt's President said, will be a "divestiture" of data[210]—or, in other words, less power for Facebook and less pollution for everyone.

CONCLUSION

Figuring out how to regulate digital firms such as Facebook, Google, and Twitter is one of the central challenges of the "Second Gilded Age,"[211] and Balkin deserves credit for moving the conversation forward. His information-fiduciary proposal, however, is also moving the conversation backward—redirecting attention away from all of the problems associated with high levels of market concentration, away from all of the problems plaguing the speech environment on social media, away from all of the problems inherent in targeted-advertising-based business models. We do not claim to know what precise mix of reform strategies is best, and the answer will likely vary across markets. But for the reasons detailed above, we believe that pro-competition policies should assume a more prominent place in the debate. By contrast, we doubt that the information-fiduciary idea should play any significant role in the struggle to rein in the dominant online platforms and reclaim the online public sphere. If this Essay's main arguments have been persuasive, the burden is on supporters of the information-fiduciary idea to clarify how it can be reconciled with the relevant firms' economic incentives and with the facts of digital life, what it adds to existing theories and practices of consumer protection, and why anyone other than the dominant platform owners should see it as a promising path forward.

---

[208] *See supra* notes 20 & 105 and accompanying text.

[209] Bundeskartellamt Press Release, *supra* note 96 (emphasis added).

[210] *Id.*

[211] *See* Balkin, *Second Gilded Age*, *supra* note 27, at 980 ("The Second Gilded Age begins, more or less, with the beginning of the digital revolution in the 1980s, but it really takes off in the early years of the commercial Internet in the 1990s, and it continues to the present day.").

Chapter 35

Discriminatory Designs on User Data
(Olivier Sylvain)

EMERGING
THREATS

DISCRIMINATORY DESIGNS ON USER DATA

BY OLIVIER SYLVAIN

KNIGHT
FIRST AMENDMENT
INSTITUTE
at Columbia University

EMERGING
THREATS

ABOUT EMERGING THREATS

The Knight First Amendment Institute's *Emerging Threats* series invites leading thinkers to identify and grapple with newly arising or intensifying structural threats to the system of free expression. These threats may be caused by changes in the forms and applications of technology, in the means and economics of communication, in the norms and practices of politics, or in legal doctrine. The papers in the series explore ways to address these threats and preserve the foundations of democracy essential to healthy open societies, including the United States.

The *Emerging Threats* series is edited by David Pozen, professor at Columbia Law School and inaugural visiting scholar at the Knight Institute.

ABOUT THE KNIGHT INSTITUTE

The Knight First Amendment Institute is a non-partisan, not-for-profit organization established by Columbia University and the John S. and James L. Knight Foundation to defend the freedoms of speech and press in the digital age through strategic litigation, research, and public education.
For more information, please visit www.knightcolumbia.org.

ABOUT THE AUTHOR

Olivier Sylvain is an Associate Professor of Law at Fordham University School of Law. He teaches legislation & regulation, administrative law, information law, and law related to communications technologies. He is also the Director of the McGannon Center for Communications Research. Additionally, Sylvain is part of a team of research engineers and social entrepreneurs to whom the National Science Foundation in fall 2017 awarded a three-year one-million-dollar grant to prototype a secure, affordable, and ener- gy-ef cient computing network that is to be owned and operated as a "commons resource" for Harlem residents. Sylvain was a Karpatkin Fellow in the National Legal Of ce of the American Civil Liberties Union in New York City and a litigation associate at Jenner & Block, LLC, in Washington, D.C. He is on the board of directors for the New York af liate of the American Civil Liberties Union.

TABLE OF CONTENTS

DISCRIMINATORY DESIGNS ON USER DATA

Olivier Sylvain

The stated aim of online intermediaries like Facebook, Twitter, and Airbnb is to provide the platforms through which users freely meet people, purchase products, and discover information.[1] As "conduits" for speech and commerce,[2] intermediaries such as these are helping to create a more vibrant and democratic marketplace for goods and ideas than any the world has seen before.[3]

That, at least, is the theory on which Congress enacted Section 230 of the Communications Decency Act (CDA) in 1996.[4] One of the central objectives of Section 230's drafters was to ensure that intermediaries are "unfettered" by the obligation to police third-party user content.[5] They believed that conventional tort principles and regulatory rules were simply not workable in an environment in which so much user content flows,[6] and they doubted that intermediaries would be able to create new value for users if they constantly had to monitor, block, or remove illicit content. In the words of free speech doctrine, members of Congress worried the intermediaries would be "chilled" by the fear that they could be held legally responsible for content posted by users.[7]

Section 230 of the CDA therefore protects intermediaries from liability for distributing third-party user content. Courts have read Section 230 broadly, creating an immunity for intermediaries who do all but "materially contribute" to the user content they distribute.[8] That is, courts have read the statute's protections to cover services that "augment[]" user content, but not services that demonstrably "help" to develop the alleged illegal expressive

+ Associate Professor, Fordham Law School.

1 *See, e.g.*, Mark Zuckerberg, *Bringing the World Closer Together*, Facebook (June 22, 2017), http://www.facebook.com/zuck/posts/10154944663901634; *About Us*, Airbnb, http://www.airbnb.com/about/about-us (last visited Feb. 23, 2018); Ricardo Castro, *A Better Way to Connect with People*, Twitter Blog (May 3, 2016), http://blog.twitter.com/official/en_us/a/2016/a-better-way-to-connect-with-people.html.

2 *Zeran v. America Online, Inc.*, 129 F.3d 327, 332 (4th Cir. 1997).

3 *See* Orly Lobel, *The Law of the Platform*, 101 Minn. L. Rev. 87, 89 (2016) (discussing "the digital platform revolution").

4 47 U.S.C. § 230 (2012).

5 *Id.* § 230(b)(2).

6 *See, e.g.*, 104 Cong. Rec. H8469 (statements of Rep. Cox and Rep. Wyden); H.R. Rep. No. 104-58, at 194 (1996); *see also* Eugene Volokh, *Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex*, 1996 U. Chi. Legal F. 377, 405–06 (1996); Alan H. Bomser, *A Lawyer's Ramble down the Information Superhighway*, 64 Fordham L. Rev. 697, 799–800 (1996).

7 *See* Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. Miami L. Rev. 137, 148 (2008); Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. Pa. L. Rev. 11, 28–29 (2006); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 Geo. Wash. L. Rev. 986, 991, 998–99, 1006–09, 1015–16 (2008); Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 Notre Dame L. Rev. 293, 300, 315–18 (2011).

8 *See, e.g.*, *Jones v. Dirty World Entm't Recordings*, 755 F.3d 398, 413 (6th Cir. 2014); *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1167–71 (9th Cir. 2008) (en banc).

9 *Roommates.com*, 521 F.3d at 1167–68.

conduct.[9] Many believe that the internet would not be as dynamic and beguiling today were it not for the protection that Section 230 has been construed to provide for online intermediaries.[10]

This may be true. But Section 230 doctrine has also had a perverse effect. By providing intermediaries with such broad legal protection, the courts' construction of Section 230 effectively underwrites content that foreseeably targets the most vulnerable among us. In their ambition to encourage an "unfettered" market for online speech, the developers of Section 230 immunity have set up a regime that makes online engagement more difficult for children, women, racial minorities, and other predictable targets of harassment and discriminatory expressive conduct. Examples abound: the gossip site that enabled users to anonymously post salacious images of unsuspecting young women;[11] the social media site through which an adult male lured a young teenage girl into a sexual assault;[12] the classifieds site that has allegedly facilitated the sex trafficking of minors;[13] the online advertising platform that allows companies to exclude Latinos from apartment rentals and older people from job postings;[14] the unrelenting social media abuse of feminist media critics[15] and a prominent black female comedian;[16] the live video stream of a gang rape of a teenage girl.[17]

The standard answer to the charge that current immunity doctrine enables these acts is that the originators of the illicit content are to blame, not the "neutral" services that facilitate online interactions.[18] Intermediaries, this position holds, merely pass along user speech; they do not encourage its production or dissemination, and, in any case, Section 230 immunity exists to protect against a different problem: the "collateral censorship" of lawful content.[19]

---

[10] *See, e.g.*, *id.* at 1180 (McKeown, J., concurring in part and dissenting in part) ("We have underscored that this broad grant of webhost immunity gives effect to Congress's stated goals 'to promote the continued development of the Internet and other interactive computer services' and 'to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services.'" (quoting *Carafano v. Metrosplash.com*, 339 F.3d 1119, 1123 (9th Cir. 2003)).

[11] *Jones v. Dirty World Entm't Recordings, LLC*, 755 F.3d 398 (6th Cir. 2014).

[12] *Doe v. MySpace,* F. Supp. 2d 843 (W.D. Tex. 2007).

[13] Doe v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016), cert. denied, 137 S. Ct. 622 (2017).

[14] Julia Angwin & Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race*, ProPublica (Oct. 28, 2016), http://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.

[15] Nick Wingfield, *Feminist Critics of Video Games Facing Threats in 'GamerGate' Campaign*, N.Y. Times (Oct. 15, 2014), http://www.nytimes.com/2014/10/16/technology/gamergate-women-video-game-threats-anita-sarkeesian.html.

[16] Anna Silman, *A Timeline of Leslie Jones's Horrific Online Abuse*, Cut (Aug. 24, 2016), http://www.thecut.com/2016/08/a-timeline-of-leslie-joness-horrific-online-abuse.html.

[17] Emanuella Grinberg, *Police: At Least 40 People Watched Teen's Sexual Assault on Facebook Live*, CNN (Mar. 22, 2017), http://www.cnn.com/2017/03/21/us/facebook-live-gang-rape-chicago/index.html.

[18] *See* Rob Goldman, This Time, ProPublica, We Disagree, Facebook Newsroom (Dec. 20, 2017), http://newsroom.fb.com/news/h/addressing-targeting-in-recruitment-ads.

[19] *See* Wu, *supra* note 7, at 315–18.

This answer, however, is either glib or too wedded to an obsolete conception of how online intermediaries operate. Intermediaries today do much more than passively distribute user content or facilitate user interactions. Many of them elicit and then algorithmically sort and repurpose the user content and data they collect. The most powerful services also leverage their market position to trade this information in ancillary or secondary markets.[20]

Intermediaries, moreover, design their platforms in ways that shape the form and substance of their users' content. Intermediaries and their defenders characterize these designs as substantively neutral technical necessities, but as I explain below, recent developments involving two of the most prominent beneficiaries of Section 230 immunity, Airbnb and Facebook, suggest otherwise. Airbnb and Facebook have enabled a range of harmful expressive acts, including violations of housing and employment laws, through the ways in which they structure their users' interactions.

At a minimum, companies should not get a free pass for enabling unlawful discriminatory conduct, regardless of the social value their services may otherwise provide. But more than this, I argue here,[21] Section 230 doctrine requires a substantial reworking if the internet is to be the great engine of democratic engagement and creativity that it should be. Section 230 is no longer serving all the purposes it was meant to serve. The statute was intended at least in part to ensure the vitality and diversity, as well as the volume, of speech on new communications platforms. By allowing intermediaries to design their platforms without internalizing the costs of the illegal speech and conduct they facilitate, however, the statute is having the opposite effect.

This paper has four parts. The first discusses the basic contours of the prevailing doctrine, including the legislative purposes behind Section 230 and the logic courts have relied on to support broad immunity for intermediaries. The second part identifies ways in which the doctrine, in assuming that intermediaries are passive disseminators of information, may accelerate the mass distribution of content that harms vulnerable people and members of historically subordinated groups. I focus in particular on the distribution of nonconsensual pornography as a species of content that not only exacts a discrete reputational or privacy toll on victims but also fuels the circulation of misogynist views that harm young women in particular.

The third part of the paper turns to the designs that intermediaries employ to structure and enhance their users' experience, and how these designs themselves can further discrimination. While the implications of this analysis reach beyond injuries to historically marginalized groups, my goal is to explain how the designs employed by two of the most prominent intermediaries today, Airbnb and Facebook, have enabled unlawful discrimination.

---

[20] *See generally* Kenneth Bamberger & Orly Lobel, *Platform Market Power*, 32 Berk. Tech. L.J. 1, 37–39 (2018) (discussing ways in which intermediaries leverage their market position to exploit user data in different markets); Lina M. Khan, Note, *Amazon's Antitrust Paradox*, 126 Yale L.J. 710 (2017) (discussing ways in which intermediaries may raise antitrust concerns to the extent they cultivate their position as "essential infrastructure" for commerce across industries).

[21] This argument builds on my recent writing. *See* Olivier Sylvain, *Intermediary Design Duties*, 50 Conn. L. Rev. 202 (2018) [hereinafter Sylvain, *Design Duties*]; Olivier Sylvain, AOL v. Zeran*: The Cyberlibertarian Hack of Section 230 Has Run Its Course*, Law.com (Nov. 10, 2017), http://www.law.com/therecorder/sites/therecorder/2017/11/10/aol-v-zeran-the-cyberlibertarian-hack-of-%C2%A7230-has-run-its-course.

The fourth and final part of the paper proposes a reform to the doctrine: I argue that courts should account for the specific ways in which intermediaries' designs do or do not enable or cause harm to the predictable targets of discrimination and harassment. As recent developments underscore, Section 230 immunity doctrine must be brought closer in line with longstanding equality and universality norms in communications law.[22]

I. Section 230 Immunity: A Brief Overview

The immunity that intermediaries enjoy under Section 230 of the CDA[23] has helped to bring about the teeming abundance of content in today's online environment. The prevailing interpretation of Section 230 bars courts from imposing liability on intermediaries that are the "mere conduits" through which user-generated content passes.[24] This doctrine protects services that host all kinds of content—everything from customer product reviews to fake news to dating profiles.

Congress invoked a very old concept when it drafted this law. The central provision of Section 230, titled "Protection for 'Good Samaritan' blocking and screening of offensive material,"[25] resembles laws in all the states that in one way or another shield defendants from liability arising from their good-faith efforts to help those in distress.[26] Good Samaritan laws are inspired by the Biblical parable that praises the do-gooder who risks ridicule and censure to help a stranger left for dead.[27]

Section 230's drafters applied this concept to online activity. They created an exception under tort law, which traditionally holds publishers liable for distributing material they know to be unlawful, but does not hold them liable if they lack notice about the illegality of the communicative act at issue.[28] Proponents of Section 230 worried that,

---

[22] On these norms, see generally Olivier Sylvain, *Network Equality*, 67 Hastings L.J. 443 (2016).

[23] The pertinent language provides as follows:
(1) Treatment of publisher or speaker
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
(2) Civil liability. No provider or user of an interactive computer service shall be held liable on account of—
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).
47 U.S.C. § 230(c) (2012). The statute excludes from immunity intermediaries that are "responsible, in whole or in part, for the creation or development" of illicit user content. *Id.* § 230(f)(3). Applying this language, courts have subjected defendant intermediaries to liability when they "materially contribute" to the offending content. *See, e.g.*, *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1167–71 (9th Cir. 2008) (en banc). In principle, the "material contribution" standard limits the scope of the protection to services that are only conduits of content. In practice, however, it is a very high bar for plaintiffs to clear.

[24] *Zeran v. America Online, Inc.*, 129 F.3d 327, 332 (4th Cir. 1997).

[25] 47 U.S.C. § 230(c).

[26] *See* Benjamin C. Zipursky, *Online Defamation, Legal Concepts, and the Good Samaritan*, 51 Val. U. L. Rev. 1, 31 (2016); Benjamin C. Zipursky, *Thinking in the Box in Legal Scholarship: The Good Samaritan and Internet Libel*, 50 J. Legal Educ. 55, 60 (2016).

[27] *Luke* 10:23-37 ("[A] Samaritan, as he traveled, came where the man was; and when he saw him, he took pity on him. He went to him and bandaged his wounds, pouring on oil and wine. Then he put the man on his own donkey, brought him to an inn and took care of him.").

[28] *Zeran*, 129 F.3d at 330–32.

without this legislation, claims for secondary liability would either stifle expressive conduct in the then-nascent medium or discourage intermediaries from policing content altogether.[29] They further insisted that government regulators such as the Federal Communications Commission should play no role in deciding what sorts of content prevailed online; viewers (and their parents) should make those decisions for themselves.[30]

While an interest in both free speech and the Good Samaritan concept drove Congress to enact Section 230, courts interpreting the statute have been far more influenced by the free speech concerns. In contrast to the nuanced requirements of the Digital Millennium Copyright Act's notice-and-takedown regime,[31] online intermediaries have not been required under Section 230 to block or screen offensive material in any particular way. Today, Section 230 doctrine provides a near-blanket immunity to intermediaries for hosting tortious third-party content. Long-established internet companies like America Online and Craigslist that host massive amounts of user content have been clear beneficiaries. Relying on Section 230, courts have immunized them from liability for everything from defamatory posts on electronic bulletin boards to racially discriminatory solicitations in online housing advertisements.[32] Leading opinions have reasoned that the scale at which third-party content passes through online services makes that content infeasible to moderate; requiring services to try would not only chill online speech but also stunt the internet's development as a transformative medium of communication.[33] This immunity now applies to a wide range of online services that host and distribute user content, including Twitter's microblogging service, Facebook's flagship social media platform, and Amazon's online marketplace. Thanks to Section 230, these companies have no legal obligation to block or remove mendacious tweets, fraudulent advertisements, or anticompetitive customer reviews by rivals.[34]

As a result, most targets of illicit online user content in the United States have little to no effective recourse under law to have that content blocked or removed. They can sue the original posters of the content. But such litigation often presents serious challenges, including the cost of bringing a lawsuit, the difficulty of discovering the identities of anonymous posters, and, even if the suit is successful on the merits, the difficulty of obtaining remedies that are commensurate with the harm.[35] Targets can also enlist services like search engine optimizers that make it harder to find the offending material. They can complain to the intermediaries about offending posts. And they can press intermediaries to improve their policies generally. If none of these strategies succeeds, users can boycott the service, as many people did recently—for one day—to protest the failure of Twitter to

[29] 104 Cong. Rec. H8469 (statement of Rep. Wyden).
[30] *Id.* (statement of Rep. Cox).
[31] *See* 17 U.S.C. § 512(c) (2012); *see also Viacom v. YouTube*, 676 F.3d 19 (2d. Cir. 2012).
[32] *See, e.g.*, *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (en banc); *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997).
[33] *See, e.g.*, *Zeran*, 129 F.3d at 333.
[34] *See, e.g.*, *Klayman v. Zuckerberg*, 753 F.3d 1354 (D.C. Cir. 2014); *Joseph v. Amazon.com*, 46 F. Supp. 3d 1095 (W.D. Wash. 2014); *Goddard v. Google*, 640 F. Supp. 2d 1193 (N.D. Cal. 2009).
[35] *See* Danielle Keats Citron, *Hate Crimes in Cyberspace* 122 (2014).

protect women from "verbal harassment, death threats, and doxing."[36] Even if effective, however, this last option sometimes feels far from optimal, given that the promise of the internet is understood to lie in its unrivaled opportunities for commercial engagement and social integration. Exit would only exacerbate extant disparities.[37]

The threat of losing consumers, it must be said, is potent enough to have moved many intermediaries to develop content-governance protocols and automated systems for content detection. Even though Section 230 doctrine has removed any legal duty to moderate third-party content, certain companies routinely block or remove content when its publication detracts from the character of the service they mean to provide. And so, for instance, Google demotes or delists search engine optimizers and sites that host "fake news" and offensive content.[38] Facebook removes clickbait articles and has now partnered with fact-checking organizations like Snopes and PolitiFact to implement a notification process for removing "fake news."[39]

The reform that the news aggregation and discussion site Reddit undertook in 2015 is especially striking in this regard. Reddit, which had been evangelical about its laissez-faire approach to user-generated content, implemented rules that ban "illegal" content, "involuntary pornography," material that "[e]ncourages or incites violence," and content that "[t]hreatens, harasses, or bullies or encourages others to do so."[40] Many "redditors" rebelled, voting up user comments that addressed Reddit's Asian-American female CEO in racist and misogynist ways.[41] These posts were popular enough among redditors to make it to the site's front page, the prime position on the site that touts itself as "the first page of the Internet." Reddit subsequently buttressed its restrictions on violent and harassing content.[42] Moreover, it recently banned a "subreddit" of self-identified misogynists.[43] Reddit's reforms have been met with fierce resistance from self-styled free speech enthusiasts.[44] But the company does not appear to be backpedaling at this time.

---

[36] *See* Debbie Chachra, *Twitter's Harassment Problem Is Baked into Its Design*, Atlantic (Oct. 16, 2017), http://www.theatlantic.com/technology/archive/2017/10/twitters-harassment-problem-is-baked-into-its-design/542952.

[37] *See Sylvain, supra note 22, at 462–64.*

[38] *See Search King v. Google*, 2003 WL 21464568 (W.D. Okla. 2003). *See generally* Deepa Seetharaman, *Google Retools Search Engine to Demote Hoaxes, Fake News*, Wall St. J. (Apr. 25, 2017), http://www.wsj.com/articles/google-retools-search-engine-to-down-play-hoaxes-fake-news-1493144451.

[39] Erin Griffith, *Facebook Can Absolutely Control Its Algorithm*, Wired (Sept. 26, 2017), http://www.wired.com/story/facebook-can-absolutely-control-its-algorithm; Amber Jamieson & Olivia Solon, *Facebook to Begin Flagging Fake News in Response to Mounting Criticism*, Guardian (Dec. 15, 2016), http://www.theguardian.com/technology/2016/dec/15/facebook-flag-fake-news-fact-check.

[40] *Reddit Content Policy*, Reddit, http://www.reddit.com/help/contentpolicy (last visited Feb. 23, 2018); *see also Removing Harassing Subreddits*, Reddit (June 10, 2015), http://np.reddit.com/r/announcements/comments/39bpam/removing_harassing_subreddits.

[41] Charlie Warzel, *Reddit Is a Shrine to the Internet We Wanted and That's a Problem*, Buzzfeed (June 19, 2015), http://www.buzzfeed.com/charliewarzel/reddit-is-a-shrine-to-the-internet-we-wanted-and-thats-a-pro.

[42] ModNews, *Update on Site-Wide Rules Regarding Violent Content*, Reddit (Oct. 25, 2017), http://www.reddit.com/r/modnews/comments/78p7bz/update_on_sitewide_rules_regarding_violent_content.

[43] *See* Aja Romano, *Reddit Just Banned One of Its Most Toxic Forums. But It Won't Touch the Donald*, Vox (Nov. 13, 2017), http://www.vox.com/culture/2017/11/13/16624688/reddit-bans-incels-the-donald-controversy.

[44] *Id.*

As this example indicates, and as new scholarship illuminates,[45] attention to consumer demand and a sense of corporate responsibility have motivated certain intermediaries to moderate certain user content. It may be tempting to conclude that reforms to Section 230 law are therefore unnecessary. Unregulated intermediaries might be the best gauges of authentic user sentiment about what is or is not objectionable. Section 230 doctrine, on this view, allows users to express and learn from each other in a dynamic fashion, without the distortions that may be caused by tort liability or government mandates. This is part of why free speech enthusiasts ascribe so much significance to the statute: Section 230 doctrine for them is premised on a noble faith in the moral and democratic power of unregulated information markets.[46]

II. The Lived Human Costs of "Unfettered" Online Speech: The Example of Nonconsensual Pornography

These arguments for near-blanket immunity only go so far, though. As much as some intermediaries may try, the fact is that many others do not make any effort to block or remove harmful expressive conduct. According to their critics, sites like Backpage (a classified site through which users are known to engage in the sex trafficking of minors) or TheDirty (a gossip site known for soliciting derogatory content about unsuspecting young women) are unabashed solicitors and distributors of a species of content that attacks members of historically subordinated groups. Under current doctrine, they are immune for acting in this way. They are just as immune under Section 230 as are ostensibly content-conscience intermediaries like Facebook and Twitter that purport to remove or block various categories of illicit user content but nevertheless sometimes distribute it.[47] The prevailing justification for this approach is to protect against the "collateral censorship" of lawful content.[48] This view holds that slippage in the direction of occasionally hosting hurtful material is the price of ensuring free speech online.

It may be correct that tolerating harmful content every now and again is the cost of promoting the statutory objective of an "unfettered" online speech environment. But just as a wide range of offline expressive acts like fraud, sexual harassment, and racially discriminatory advertisements for housing are not entitled to legal protection, we might wonder whether online services should be entirely immune for similar behaviors by their users.[49] To be

[45] *See* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 113 Harv. L. Rev. (forthcoming 2018), http://ssrn.com/abstract=2937985 (manuscript at 32–37); Karen Levy & Solon Barocas, *Designing Against Discrimination in Online Markets*, 32 Berkeley Tech. L.J. (forthcoming 2018), http://ssrn.com/abstract=3084502.

[46] *See* Derek Khanna, *The Law That Gave Us the Modern Internet—and the Campaign to Kill It*, Atlantic (Sept. 12, 2017), http://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-internet-and-the-campaign-to-kill-it/279588.

[47] *See, e.g.*, Ariana Tobin et al., *Facebook's Uneven Enforcement of Hate Speech Rules Allows Vile Posts to Stay Up*, ProPublica (Dec. 27, 2017), http://www.propublica.org/article/facebook-enforcement-hate-speech-rules-mistakes; Julia Angwin et al., *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, ProPublica (Nov. 21, 2017), http://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

[48] *See* sources cited *supra* note 7.

[49] There also is a toll on the human moderators responsible for censoring illicit content. Recent reporting suggests that these workers are traumatized by the material they censor. *See* Lauren Weber & Deepa Seetharaman, *The Worst Job in Technology: Staring at Human Depravity to Keep It off Facebook*, Wall St. J. (Dec. 27, 2017), http://www.wsj.com/articles/the-worst-job-in-technology-staring-at-human-depravity-to-keep-it-off-facebook-1514398398.

sure, there is a significant qualitative and quantitative difference between the reach of offline and online expressive acts: The latter travel further and faster than the former by a long shot. But this fact hardly removes the need to regulate harmful online behaviors. Quite the contrary. The human costs of "unfettered" online speech may be aggravated by the internet's reach, and the costs themselves are disproportionately shouldered by those who are most likely to be the targets of attacks and abuse both online and off. That is to say, the victims of online abuse tend to be the same sorts of people who have always been subject to attack and harassment offline in the United States and elsewhere—in particular, young women, racial minorities, and sexual "deviants."[50]

The harm that these users experience is made worse by the way in which illicit or inflammatory content, once distributed, can spread across the internet at a speed and scale that is hard, if not impossible, to control. This unforgiving ecology raises the stakes of occasional slippage for the predictable targets and systemic victims of harmful content. The internet thus reinforces some of the classic arguments for the regulation of assaultive speech acts that target members of historically subordinated groups.[51] The vitriolic content that flows through online intermediaries affects members of these groups distinctively, discouraging them from participating fully in public life online and making their social and commercial integration even more difficult than it might otherwise be.[52]

Consider nonconsensual pornography, the distribution of nude images of a person who never authorized their distribution. On the internet, such images are generally shared in order to humiliate or harass the depicted person. In some instances, third parties then exploit the images to extort the victim, as in the case of sites that require a fee to take the images down.[53] Other parties discover and distribute such images for free, without necessarily knowing anything about the depicted individual.

The injuries caused by nonconsensual pornography are clear and are felt most immediately and painfully by its victims. Section 230 jurisprudence is riddled with cases that illustrate these harms. In one of the more cited ones, *Barnes v. Yahoo!, Inc.*,[54] a young woman sued Yahoo! for failing to remove a false dating site profile of her created by her ex-boyfriend. The profile contained her work phone number and address, as well as nude and suggestive photographs accompanied by promises of sex. Would-be suitors and predators soon came looking for her at work. The harm caused by this cruel hoax was plain.

---

[50] *See* Citron, *supra* note 35, at 13–16.

[51] *See, e.g.*, Mari J. Matsuda et al., *Words that Wound: Critical Race Theory, Assaultive Speech, and the First Amendment* (1993); Charles R. Lawrence, III, *Crossburning and the Sound of Silence: Antisubordination Theory and the First Amendment*, 37 Vill. L. Rev. 787 (1992).

[52] *Cf.* Richard Delgado & Jean Stefancic, *Understanding Words that Wound* 217–18 (2004) (advocating a "new approach" that "points out how speech and equality stand in reciprocal relation; neither can thrive without the other. Speech without equality is a lecture, a sermon, a rant. Speech, in other words, presumes equality, or something like it, among participants in a dialogue").

[53] *See* Margaret Talbot, *The Attorney Fighting Revenge Porn*, New Yorker (Dec. 5, 2016), http://www.newyorker.com/magazine/2016/12/05/the-attorney-fighting-revenge-porn.

[54] 570 F.3d 1096 (9th Cir. 2009).

Victims of nonconsensual pornography may experience many other indignities. Once posted, the offending image takes on a life of its own, exacting something that resembles an endlessly repeating privacy invasion. Danielle Citron and Mary Anne Franks, who have been thinking and writing compellingly about the issue for almost a decade now, explain the phenomenon:

> Today, intimate photos are increasingly being distributed online, potentially reaching thousands, even millions of people, with a click of a mouse. A person's nude photo can be uploaded to a website where thousands of people can view and repost it. In short order, the image can appear prominently in a search of the victim's name. It can be e-mailed or otherwise exhibited to the victim's family, employers, coworkers, and friends. The Internet provides a staggering means of amplification, extending the reach of content in unimaginable ways.[55]

The scale of distribution magnifies the harm to depicted individuals far beyond what is possible through other communications technologies. In this environment, taking down nonconsensual pornography, once it has been posted on an online intermediary, often becomes a futile and agonizing game of whack-a-mole.

In addition to the direct harms to those whose images are being exploited, the distribution of nonconsensual pornography also exacts a more general harm that mirrors and reinforces the routine subjugation of young women.[56] It is different in this regard from defamatory user posts, the prototypical subject of Section 230 jurisprudence, in which the injury caused by the defamatory posts are reputational in nature.[57] Nonconsensual pornography sweeps its victims into a network of blogs, pornography sites, social media groups, Tumblrs, and Reddit discussion threads that enthusiastically traffic in the collective humiliation of young women.[58]

And yet, Section 230 doctrine relieves online intermediaries of any legal obligation to block or remove nonconsensual pornography. When sued for distributing such images and videos, the intermediaries cite Section 230 to justify their passive role. Courts have generally sided with them, explaining that the immunity is not contingent on sites' policing of illicit user content.[59] The result is not only grief for the predictable victims of online abuse and harassment but also a regulatory regime that helps to reinforce systemic subordination.

---

[55] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. 345, 350 (2014).

[56] *See* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 Mich. L. Rev. 373 (2009); *see also* Clare McGlynn et al., *Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse*, 25 Feminist Legal Stud. 25 (2017); Catherine Buni & Soraya Chemaly, *The Unsafety Net: How Social Media Turned Against Women*, Atlantic (Oct. 9, 2014), http://www.theatlantic.com/technology/archive/2014/10/the-unsafety-net-how-social-media-turned-against-women/381261.

[57] *See, e.g.*, *Barrett v. Rosenthal*, 146 P.3d 510 (Cal. 2006); *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003); *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997). *See generally* Joel R. Reidenberg et al., Ctr. on Law & Info. Pol'y at Fordham Law Sch., *Section 230 of the Communications Decency Act: A Survey of the Legal Literature and Reform Proposals* (Apr. 25, 2012), http://ssrn.com/abstract=2046230 (surveying sixteen years of Section 230 cases).

[58] *See* Citron, *supra* note 35, at 127 ("Cyber harassment reinforces gender stereotypes by casting women as sex objects that are unfit for life's important opportunities.").

[59] *See, e.g.*, *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009); *Jones v. Dirty World Entm't Recordings, LLC*, 755 F.3d 398 (6th Cir. 2014).

III. More than a Conduit: Online Intermediaries' Designs on User Data

As pernicious as it is, cyberharassment does not reflect the full scope of the threat that such broad legal protection for online intermediaries poses to vulnerable persons. This is because, today, most if not all intermediaries affirmatively shape the form and substance of user content. Adding to the arguments that scholars like Citron and Franks have ably made, I want to call attention here to this crucial way in which Section 230 immunity entrenches extant barriers to social and commercial integration for historically subordinated groups. I want to suggest, furthermore, that over two decades into the development of the networked information economy, online intermediaries should not be able to claim blissful indifference when their designs predictably elicit or even encourage expressive conduct that perpetuates discrimination and subjugation.

I make these arguments in this part in several sections. In section A, I illustrate the ways in which intermediaries pervasively influence users' online experiences. In section B, I explain how such designs can enable and exacerbate certain categories of harmful expressive acts. Section C looks at the courts' responses.

A. Intermediary Designs and User Experiences

Popular services like Facebook, Twitter, and Airbnb offer good examples of how intermediary designs interact with user experiences. Twitter immediately distributes its users' posts (tweets) after the users type them. But its user interface affects the nature and content of those tweets. Twitter's 280-character limitation, for example, has generated its own abbreviated syntax and conventions (for example, hashtags and subtweets).[60] The company also allows pseudonyms, effectively allowing users to be anonymous. This liberal approach to attribution invites creativity and useful provocation but also the harassment and targeted attacks mentioned above. Twitter knows this, and in many cases it will take down such attacks after the fact and remove users who routinely violate the company's no-harassment policy.

These superficial interface design features are distinct from the designs on content that occur behind (so to speak) the user interface. Some companies are intentionally deceptive about how they acquire or employ content. Take, for example, the online marketing company that placed deceptive information about its clients' products on affiliated "fake news" sites.[61] Or consider the online sleuthing company that, in response to solicited user requests for information about people, routinely contracted with third-party researchers to retrieve information in ways it allegedly knew violated privacy law.[62]

[60] Twitter recognizes the significance of its character limitation; it increased the limitation from 140 in November 2017 to improve the user experience. *See* Aatif Sulleyman, *Twitter Introduces 280 Characters to All Users*, Independent (Nov. 7, 2017), http://www.independent.co.uk/life-style/gadgets-and-tech/news/twitter-280-characters-tweets-start-when-get-latest-a8042716.html.
[61] *See FTC v. LeadClick Media*, 838 F.3d 158 (2d Cir. 2016).
[62] *See FTC v. Accusearch*, 570 F.3d 1187 (10th Cir. 2009).

Without necessarily resorting to outright deception, many more intermediaries administer their platforms in obscure or undisclosed ways that are meant to influence how users behave on the site.[63] Many intermediaries, for example, employ user interfaces designed to hold user attention by inducing something like addictive reliance.[64] Facebook employs techniques to ensure that each user sees stories and updates in her "News Feeds" that she may not have seen on her last visit to site.[65] And its engineers constantly tweak the algorithms that manage the user experience.[66] In addition, many intermediaries analyze, sort, and repurpose the user content they elicit. Facebook and Twitter, for example, employ software to make meaning out of their users' "reactions," search terms, and browsing activity in order to curate the content of each user's individual feed, personalized advertisements, and recommendations about "who to follow." (A *Wired* magazine headline of three years ago comes to mind: "How Facebook Knows You Better than Your Friends Do."[67]) Intermediaries ostensibly do all of these things to improve user experiences, but their practices are often problematic and opaque to the outside world.[68] As very recent revelations involving Cambridge Analytica underscore, Facebook for years shared its unrivaled trove of user data with third-party researchers, application developers, and data brokers in the interest of deepening user engagement.[69] Facebook reportedly took 30 percent of developer profits in the process.[70]

This is all to say that intermediaries now have near-total control of users' online experience. They design and predict nearly everything that happens on their site, from the moment a user signs in to the moment she logs out. The lure of "big" consumer data pushes them to be ever more aggressive in their efforts to attract new users, retain existing users, and generate information about users that they can mine and market to others. It is neither surprising nor troubling that companies make handsome profits in this way. But these developments undermine any notion that online intermediaries deserve immunity because they are mere conduits for, or passive publishers of, their users' expression. Online intermediaries pervasively shape, study, and exploit communicative acts on their services.

---

[63] *See* Frank Pasquale, *The Black Box Society* 3, 28–31 (2015).

[64] *See* Adam Alter, *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked* (2017); Paul Lewis, *Our Minds Can Be Hijacked: The Tech Insiders Who Fear a Smartphone Dystopia*, Guardian (Oct. 6, 2017), http://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia. *See generally* Tim Wu, *The Attention Merchants: The Epic Scramble to Get Inside Our Heads* (2016); Nir Eyal, *Hooked: How to Build Habit-Forming Products* (2014).

[65] Noam Cohen, *Silicon Valley Is Not Your Friend*, N.Y. Times (Oct. 13, 2017), http://www.nytimes.com/interactive/2017/10/13/opinion/sunday/Silicon-Valley-Is-Not-Your-Friend.html.

[66] Julia Carrie Wong, *Facebook Overhauls News Feed in Favor of 'Meaningful Social Interactions,'* Guardian (Jan. 11, 2018), http://www.theguardian.com/technology/2018/jan/11/facebook-news-feed-algorithm-overhaul-mark-zuckerberg.

[67] Issie Lapowsky, *How Facebook Knows You Better Than Your Friends Do*, Wired (Jan. 13, 2015), http://www.wired.com/2015/01/facebook-personality-test.

[68] *See* Christina Passariello, *Facebook: Media Company or Technology Platform?*, Wall St. J. (Oct. 30, 2016), http://www.wsj.com/articles/facebook-media-company-or-technology-platform-1477880520.

[69] *See* Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), http://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; *see also* Paul Lewis, *'Utterly Horrifying': Ex-Facebook insider Says Covert Data Harvesting Was Routine*, Guardian (Mar. 20, 2018), http://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

[70] Lewis, *supra* note 69.

All of this, moreover, belies the old faith that such services operate at too massive a scale to be asked to police user content. Online intermediaries are already carefully curating and commoditizing this content through automated "black box" processes that would seem unworkable were they not working so well. The standard justifications for broad immunity under Section 230—grounded in fears of imposing excessive burdens on intermediaries and chilling their distribution of lawful material—have become increasingly divorced from technological and economic realities. As intermediaries have figured out how to manage and distribute user data with ever greater precision, the traditional case for Section 230 immunity has become ever less compelling, if not altogether inapt.

B. Discriminatory Designs on User Content and Data: The Example of Online Housing Marketplaces

These developments in intermediary design have been underway for over a decade now and have become far-reaching and consequential enough in themselves to warrant rethinking of Section 230 doctrine. The problems with the doctrine, however, are made worse when intermediaries' designs facilitate expressive conduct that harms vulnerable people and members of historically subordinated groups.[71] We often hear about the dangerous content that intermediaries automatically distribute by algorithm, as in the notorious ways in which Facebook and Twitter facilitated the targeted dissemination of "fake news" in the months leading up to the 2016 presidential election,[72] or the advertisement that Instagram made of a user's personal photo of a violently misogynist threat she had received through her account.[73] My point here, however, is that the stakes of automated intermediary designs are especially high for certain predictable communities. Unpoliced, putatively neutral online application and service designs can entrench longstanding racial and gender disparities.

Consider Airbnb's popular home-sharing service. Quite unlike Twitter's liberal approach to personal attribution, Airbnb's main service requires each guest to create an online profile with certain information, including a genuine name and phone number. It also encourages inclusion of a real photograph.[74] For Airbnb, the authenticity of this profile information is vital to the operation of the service, as it engenders a sense of trust and connection between hosts and guests. Guests' physical characteristics may contain social cues that instill either familiarity and comfort, on the one hand, or suspicion and distrust, on the other. The sense of authentic connection that Airbnb is adamant about cultivating, however, has dangerous consequences in a market long plagued by discrimination against racial and ethnic minorities. In its more insidious manifestations, access to a guest's name and profile picture affords hosts the ability to assess the trustworthiness of a guest based on illicit biases—against, say, Latinos or blacks—that do not accurately predict a prospective guest's reliability as a tenant. In this way, Airbnb's service directly reinforces discrimination when it requires users to share information that suggests their own race.

---

[71] *Cf.* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 Calif. L. Rev. 671 (2016) (discussing ways in which algorithmic analysis and machine learning may produce discriminatory impacts); Levy & Barocas, *supra* note 45 (discussing ways in which intermediary designs may have discriminatory impacts).

[72] *See, e.g.*, Nancy Scola & Josh Meyer, *Twitter Takes Its Turns in the Russian Probe Spotlight*, Politico (Sept. 28, 2017), http://www.politico.com/story/2017/09/28/twitter-russia-probe-spotlight-243239.

[73] Sam Levin, *Instagram Uses 'I Will Rape You' Post as Facebook Ad in Latest Algorithm Mishap*, Guardian (Sept. 21, 2017), http://www.theguardian.com/technology/2017/sep/21/instagram-death-threat-facebook-olivia-solon.

[74] Airbnb also gives users the option of importing information from users' Facebook accounts.

That race would matter so much to Airbnb hosts should not be a surprise. Race, after all, has long played an enormous—and pernicious—role in U.S. housing markets, online as well as offline. SketchFactor, the crowdsourced neighborhood safety rating application, for example, became little more than a platform for users to share racist stereotypes about "shady" parts of town.[75] Match.com, the ostensibly race-neutral online dating application, facilitates users' discrimination against blacks.[76] Similarly, Airbnb hosts use the home-sharing service to discriminate against racial minorities whose identities as such are suggested in their profiles. Guests have complained publicly about this phenomenon, giving rise to the hashtag #AirbnbWhileBlack.[77] One guest reported that a host abruptly cancelled her reservation after sending an unambiguously bigoted explanation: "I wouldn't rent to u if u were the last person on earth. One word says it all. Asian."[78] Researchers at the Harvard Business School have substantiated individual claims like these, finding that Airbnb guests "with distinctively African-American names are 16 percent less likely to be accepted relative to identical guests with distinctively White names."[79] Airbnb felt compelled to commission a well-regarded civil rights attorney to conduct a study on the topic. Her review, too, found a distinct pattern of host discrimination against users whose profiles suggest they are a member of a racial minority group.[80]

The difference between these racially discriminatory patterns as they appear on Airbnb versus dating or neighborhood rating apps is that the former are illegal because they violate fair housing laws. The 1968 Fair Housing Act (FHA), for example, specifically forbids home sellers or renters, as well as brokers, property managers, and agents, from distributing advertisements "that indicate[] any preference, limitation, or discrimination based on race, color, religion, sex, handicap, familial status, or national origin."[81] States have similar laws. In light of the mounting evidence that hosts use its service to discriminate unlawfully, Airbnb has augmented its efforts to police discriminatory behavior by hosts. In addition to requiring users to forswear that practice, the company now also requires new users to agree "to treat everyone in the Airbnb community—regardless of their race, religion, national origin, ethnicity, skin color, disability, sex, gender identity, sexual orientation or age—with

[75] Andrew Marantz, *When an App Is Called Racist*, New Yorker (July 29, 2015), http://www.newyorker.com/business/currency/what-to-do-when-your-app-is-racist. *See generally* Anthony G. Greenwald & Linda Hamilton Krieger, *Implicit Bias: Scientific Foundations*, 94 Calif. L. Rev. 945 (2006); Jerry Kang & Kristin Lane, *Seeing through Colorblindness: Implicit Bias and the Law*, 58 UCLA L. Rev. 465 (2010).
[76] *See* Emanuella Grinberg, *When It Comes to Dating Sites, Race Matters*, CNN (Jan. 13, 2016), http://www.cnn.com/2016/01/13/living/where-white-people-meet-feat/index.html. This is to say nothing of sites like WhereWhitePeopleMeet that openly exploit this phenomenon. *Id.*
[77] *See, e.g.*, Kristen Clarke, *Does Airbnb Enable Racism?*, N.Y. Times (Aug. 23, 2016), http://www.nytimes.com/2016/08/23/opinion/how-airbnb-can-fight-racial-discrimination.html; Carla Javier, *A Trump-Loving Airbnb Host Canceled This Woman's Reservation Because She's Asian*, Splinter News (Apr. 6, 2017), http://splinternews.com/a-trump-loving-airbnb-host-canceled-this-womans-reserva-1794086239; Carla Herreria, *Amsterdam Airbnb Host Accused of Pushing South African Down Stairs Is Arrested*, Huffington Post (July 13, 2017), http://www.huffingtonpost.com/entry/amsterdam-airbnb-host-pushes-guest-stairs-racist_us_59680a7de4b03389bb164286.
[78] Javier, *supra* note 78.
[79] Benjamin Edelman et al., *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 Am. Econ. J.: Applied Econ. 1, 2 (2017).
[80] Laura Murphy, Laura Murphy & Assocs., *Airbnb's Work to Fight Discrimination and Build Inclusion: A Report Submitted to Airbnb* 16–17 (2016), http://blog.atairbnb.com/wp-content/uploads/2016/09/REPORT_Airbnbs-Work-to-Fight-Discrimination-and-Build-Inclusion.pdf.
[81] 42 U.S.C. § 3604(c) (2012).

respect, and without judgment or bias."[82] Airbnb has also promoted its "instant bookings" service as an alternative to its main service.[83] "Instant bookings" does not require elaborate profiles (including racially suggestive names or pictures) to complete transactions.

However, Airbnb still facilitates discrimination through its main service to the extent that it continues to rely on names and pictures. The "instant bookings" feature, paired with the main service, creates a "two-tiered reservations system": In one system (instant bookings), guests lose a sense of conviviality with hosts but obtain some peace of mind in knowing that they will not be discriminated against on the basis of race, while in the other system (the main service), discrimination is inevitable but also exploited to promote "authentic" connections.[84]

Section 230 doctrine arguably insulates Airbnb's design choices from antidiscrimination law's scrutiny. The company and its defenders have routinely cited Section 230 as a protection against liability for a wide range of illicit host activities, including discrimination that violates fair housing laws.[85] In their view, the statutory immunity is robust enough to protect Airbnb from liability for these expressive acts by third-party hosts because the company only facilitates transactions between users.[86] It does not contribute anything material to the transactions themselves.[87]

Airbnb is far from alone in deploying designs that routinely generate serious forms of discrimination. Late in 2016, ProPublica published the first in a series of illuminating reports on Facebook Ads, the social media company's powerful microtargeted advertising platform. This service enables advertisers to customize campaigns to social media users based on the information that Facebook gathers about those users. Facebook Ads is a bargain (at a clip of $30 for each advertisement) compared to the going rate of top social media marketing and advertising firms. It can be a great help to entrepreneurs of all sizes because it identifies salient market segments in real time.

Facebook Ads is also distinctive because the company employs software, first, to analyze the unrivaled troves of user data that it collects and, second, to create dozens of categories from which advertisers may choose. These include targeted classifications within geographic locations, demographics, friendship networks, and online user

---

[82] Airbnb, *General Questions About the Airbnb Community Commitment*, http://www.airbnb.com/help/article/1523/general-questions-about-the-airbnb-community-commitment (last visited Feb. 23, 2018).

[83] Airbnb, *Business Is Better with Instant Book*, http://www.airbnb.com/host/instant (last visited Feb. 23, 2018).

[84] Katie Benner, *Airbnb Adopts Rules to Fight Discrimination by Its Hosts*, N.Y. Times (Sept. 8, 2016), http://www.nytimes.com/2016/09/09/technology/airbnb-anti-discrimination-rules.html. As Nancy Leong and Aaron Belzer have recently shown, moreover, the guest-rating systems on online platforms like Airbnb and Uber further entrench discrimination by aggregating illicit biases over time. *See* Nancy Leong & Aaron Belzer, *The New Public Accommodations: Race Discrimination in the Platform Economy*, 105 Geo. L.J. 1271, 1293–95 (2017).

[85] Tracey Lien, *Airbnb's Legal Argument: Don't Hold Us Accountable for the Actions of Our Hosts*, L.A. Times (June 29, 2016), http://www.latimes.com/business/technology/la-fi-tn-airbnb-free-speech-20160629-snap-story.html.

[86] *Id.*; see also Julia Carrie Wong, *How a Failed Attempt to Get Porn off the Internet Protects Airbnb from the Law*, Guardian (June 29, 2016), http://www.theguardian.com/technology/2016/jun/29/airbnb-lawsuit-san-francisco-regulation-internet-porn.

[87] On the other hand, Airbnb's decision to settle in some of these cases may suggest that the company worries about its role in perpetuating discrimination, irrespective of whether Section 230 supplies immunity. *Cf.* Sam Levin, *Airbnb Gives in to Regulator's Demand to Test for Racial Discrimination by Hosts*, Guardian (Apr. 27, 2017), http://www.theguardian.com/technology/2017/apr/27/airbnb-government-housing-test-black-discrimination.

behaviors.[88] Among the more notorious categories in the recent past were ones that "enabled advertisers to direct their pitches to the news feeds of almost 2,300 people who expressed interest in the topics of 'Jew hater,' 'How to burn jews,' or 'History of "why jews ruin the world."'"[89] No human at Facebook created these specific anti-Semitic classifications. Facebook's algorithms determined that they were salient based on user interest at the time.[90]

Facebook's algorithms likewise seem to have created various controversial demographic classifications for "ethnic" or "multicultural" affinities, a category that does not connote race as such so much as users' cultural associations and inclinations.[91] These classifications are predictive proxies, however, for race and ethnicity. Recent news reports have shown that, through these classifications, Facebook Ads has enabled building managers and employers to exclude racial minorities from advertisements about apartment rentals and to exclude older people from advertisements about jobs.[92] When faced with stories of discrimination on the advertising platform in late 2016, Facebook immediately announced a plan to stamp out the practice.[93] Among other things, Facebook now requires advertisers to certify that they do not discriminate in contravention of civil rights laws.[94] But, as with Airbnb, reports of illicit use of the site continue to surface.[95]

Critics and victims of these practices would greatly prefer to seek relief and reform from the intermediary itself—from Facebook—rather than from thousands of individual users. Aggrieved parties have thus filed federal class action lawsuits against Facebook alleging fair housing and employment discrimination violations.[96] Predictably, Facebook has cited Section 230 to defend its advertising platform. It argues that the company does not control the reach or content of targeted ads; third-party advertisers do. According to Facebook, its platform is nothing more than a "neutral tool" to help these advertisers "target their ads to groups of users most likely to be interested in the goods or services being offered."[97] This activity, it asserts, falls squarely in the category of "publishing" for which companies like Facebook are granted immunity under the CDA.

---

[88] *See* Facebook Business, *Facebook Ads*, http://www.facebook.com/business/products/ads (last visited Feb. 23, 2018).

[89] Julia Angwin et al., *Facebook Enabled Advertisers to Reach 'Jew Haters,'* ProPublica (Sept. 14, 2017), http://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters.

[90] Jaclyn Peiser, *Anti-Semitism's Rise Gives the Forward New Resolve*, N.Y. Times (Oct. 8, 2017), http://www.nytimes.com/2017/10/08/business/media/the-forward-antisemitism.html.

[91] ProPublica, which first broke the story about this practice, *see* Angwin & Parris, *supra* note 14, has not reported on whether Facebook generates these categories manually or by algorithm. I do not take up the question here, but the roles of automation and machine learning raise difficult questions about proof of intention under current nondiscrimination law.

[92] *See* Julia Angwin et al., *Facebook Job Ads Raise Concerns About Age Discrimination*, N.Y. Times (Dec. 20, 2017), http://www.nytimes.com/2017/12/20/business/facebook-job-ads.html; Angwin & Parris, *supra* note 14.

[93] Sapna Maheshwari & Mike Isaac, *Facebook Will Stop Some Ads from Targeting Users by Race,* N.Y. Times (Nov. 11, 2016), http://www.nytimes.com/2016/11/12/business/media/facebook-will-stop-some-ads-from-targeting-users-by-race.html.

[94] Rachel Goodman, *Facebook's Ad Targeting Problems Prove How Easy It Is to Discriminate Online*, NBC News (Nov. 30, 2017), http://www.nbcnews.com/think/opinion/facebook-s-ad-targeting-problems-prove-how-easy-it-discriminate-ncna825196.

[95] *Id.*

[96] *See, e.g.*, Complaint, *Mobley v. Facebook, Inc.*, No. 5:16-cv-06440-EJD (N.D. Cal. Nov. 3, 2016), 2016 WL 6599689. cause substantial emotional distress." 18 U.S.C § 2261A(2)(B).

[97] Defendant's Notice of Motion and Motion to Dismiss First Amendment Complaint; Memorandum of Points and Authorities in Support Thereof at 10, *Mobley v. Facebook, Inc.* (N.D. Cal.) (June 1, 2017) (No. 5:16-cv-06440-EJD), *available at* http://assets.documentcloud.org/documents/4333515/Outten-FB-FB-Motion-to-Dismiss-4-3-17.pdf. Facebook also asserts that the plaintiffs lack standing and that, in any event, it is not discriminating within the meaning of the pertinent civil rights laws. *Id.* at 14–25.

C. Doctrinal Responses—and Resources

Section 230 doctrine could very well lead courts to side with Facebook on this matter. But it is hardly obvious that it should, given that the alleged discrimination would not be possible but for the way in which Facebook leverages its unrivaled access to social media user data to generate the illicit categories. In Facebook's favor, courts have read Section 230 to immunize intermediaries that host racially discriminatory advertisements or solicitations. In 2008, the U.S. Court of Appeals for the Seventh Circuit explained that the popular classifieds site Craigslist could not be held liable for hosting third-party housing advertisements that overtly expressed preferences for people on the basis of race, sex, religion, sexual orientation, and family status.[98] The panel explained that Congress enacted the statute to protect services exactly like Craigslist. The company neither had a hand in the authorship of the discriminatory advertisements nor caused or induced advertisers to post such content.[99] Craigslist, the panel reasoned, acts as nothing more than a publisher of (sometimes racist) user content and, as such, could not be liable under federal fair housing law.[100] Had Congress meant to include an exception under Section 230 for such laws, it would have said so.[101]

But the Section 230 case law also contains some resources and opportunities for plaintiffs like those in the current Facebook Ads case. In the same year that the Seventh Circuit ruled in favor of Craigslist, the Ninth Circuit sitting *en banc* held that an important design element of Roommates.com, a website that also brokers connections between people in the housing market, was not immune under Section 230.[102] As a condition of participation on the site, Roommates.com required subscribers to express preferences that are strictly forbidden under fair housing law.[103] Among other things, the site's developers designed a dropdown menu that listed gender, sexual orientation, and family status as potential options. (Notably, the menu did not include race among the listed items.) A participant had to share such a preference to find a match. The Ninth Circuit held that this design feature "materially contributed" to a fair housing law violation every time a user expressed a preference for one of those prohibited classifications.[104] This conclusion flowed from language in Section 230 that does not extend protection to intermediaries that help to "create or develop" illicit third-party content.[105]

As important as the *Roommates.com* opinion has become in limiting the scope of immunity under Section 230, it is worth noting that the Ninth Circuit was very careful in how it discussed its holding. The court made a point of limiting its no-immunity conclusion to the dropdown menu. The plaintiffs had argued that a separate,

---

[98] *Chicago Lawyers' Comm. for Civil Rights v. Craigslist, Inc.*, 519 F.3d 666 (7th Cir. 2008).
[99] *Id.* at 671.
[100] *Id.*
[101] *Id.*
[102] *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008) (en banc).
[103] *Id.* at 1165–72.
[104] *Id.*
[105] 47 U.S.C. § 230(f)(3) (2012). After remand, a three-judge panel did nothing to alter this conclusion in its ruling four years later. *Fair Hous. Council of San Fernando Valley v. Roommate.com, LLC*, 666 F.3d 1216 (9th Cir. 2012). In this later opinion, the panel held that, while the immunity under Section 230 did not bar the suit against Roommates.com for its drop-down menu, Roommates.com's specific conduct at issue did not violate the FHA because "the FHA doesn't apply to the sharing of living units" as opposed to "the sale or rental of a dwelling." *Id.* at 1222 (discussing the scope of 42 U.S.C. § 3604(c)).

blank dialogue box that Roommates.com makes available to subscribers also permits them to express bigoted preferences and share information in violation of fair housing law.[106] For example, subscribers had posted comments that they "prefer white Male roommates," that "the person applying for the room MUST be a BLACK GAY MALE," or that they are "NOT looking for black muslims."[107] The court held that Section 230 immunizes Roommates.com from liability for statements like these. It is not enough, the court reasoned, that the site encourages subscribers to share preferences and information, as this is "precisely the kind of situation for which section 230 was designed to provide immunity."[108] Roommates.com only "passively displayed" the statements and had "no way to distinguish unlawful discriminatory preferences from perfectly legitimate statements."[109] This conclusion jibes with the Seventh Circuit's approach to Craigslist.[110] Indeed, these two opinions neatly mapped out the basic contours of Section 230 doctrine when they were decided in 2008. The *Roommates.com* opinion, in particular, is now routinely cited as authority for the "material contribution" standard.[111]

The Ninth Circuit's other notable conclusion in that case, decided a couple of years after a post-remand trial court finding for Roommates.com, was that the plaintiff civil rights organization, the Fair Housing Council of the San Fernando Valley (FHC), had standing to seek relief even if it was not itself the victim of a discrete discriminatory act.[112] FHC had alleged that Roommates.com was strictly liable for designing its site in a way that discriminated against prospective renters. It claimed standing to sue, however, because its research into the company's discriminatory designs was a drain on its resources and frustrated its mission.[113] The Ninth Circuit agreed, holding that FHC had suffered an actual injury sufficient to have standing.

In essence, the court determined that the organization could stand in for a hypothetical Roommates.com subscriber who would be harmed by users' discriminatory preferences and postings.[114]
This holding makes good sense, as discriminatory targeted advertisements and solicitations subjugate racial minorities even when their victims do not witness or otherwise experience the discriminatory act directly.
Civil rights laws often reach beyond discrete acts of exclusion in order to redress systemic patterns of subordination and exclusion. Roommates.com's design choices, FHC had argued, facilitated communicative acts of discrimination in a market long plagued by that very problem. And if not for FHC's intervention, the court reasoned, these patterns of bias would continue.

---

[106] *Roommates.com*, 521 F.3d at 1173.
[107] *Id.*
[108] *Id.* at 1174.
[109] *Id.*
[110] *See id.* at 1173 n.33 (explaining that the court's holding is consistent with the Seventh Circuit's *Craigslist* opinion).
[111] *See, e.g.*, *Jones v. Dirty World Entm't Recordings*, 755 F.3d 398, 410–12 (6th Cir. 2014); *FTC v. Accusearch*, 570 F.3d 1187, 1200 (10th Cir. 2009).
[112] *Fair Hous. Council of San Fernando Valley v. Roommate.com, LLC*, 666 F.3d 1216, 1219 (9th Cir. 2012).
[113] *Id.*
[114] *Id.*

IV. Toward a More Nuanced Immunity Doctrine

The *Roommates.com* opinion, issued a decade ago, helps to show the way forward. The Ninth Circuit's careful treatment of the two contested features of the website design of Roommates.com demonstrated an appreciation for the diversity of ways in which the company elicits content from users, and its standing ruling demonstrated an appreciation for the realities of civil rights harms.

However, the Ninth Circuit's opinion did not go far enough; it did not address the increasingly subtle and tentacular kinds of control that online intermediaries exert over users' experiences today. The system through which Facebook, for example, algorithmically sorts and repurposes user data to support microtargeted advertising is a far cry from the clumsy dropdown menu in the *Roommates.com* case. Two decades after the CDA's enactment, it has become increasingly implausible to equate this powerful manipulation of users' data and content with traditional publishing under Section 230.

Section 230 doctrine must be adapted to the political economy of contemporary online information flows. Judges and litigants already have a rich set of tools from antidiscrimination and consumer protection law for determining liability and providing remedies for harmful expressive conduct. But the current Section 230 doctrine cuts cyberspace off from these other bodies of law, foreclosing liability analysis for companies whose service designs routinely facilitate or even encourage illicit content.

It is important to emphasize, moreover, that holding intermediaries to account for such designs does not require anything like strict liability for the harms caused by nonconsensual pornography or any other user-generated content. Consistent with the neglected Good Samaritan goal of the statute, Section 230 can quite comfortably be interpreted to provide a safe harbor for intermediaries that try in good faith to block or take such content down.[115] That is, after all, precisely what the text of Section 230(c)(2)(A) says, at least with regard to "objectionable" speech.[116] At the same time, courts could allow plaintiffs to seek redress from intermediaries that knowingly or negligently facilitate the distribution of harmful content. As the Ninth Circuit's ruling against Roommates.com shows, we do not need new statutory language to assess intermediary liability when the user interface at issue enables illegal online conduct.

But the experience of two decades of Section 230 litigation does suggest that new statutory language could help, particularly since the prevailing view prevents the plain meaning of the Good Samaritan title and Section 230(c)(2)(A) from doing any meaningful work. The statute itself, moreover, fails to give clear direction on the kinds of torts it covers. Nor, for that matter, does the statute address the extent to which a defendant must "create[] or develop[]"

---

[115] *See* Facebook Business, *Take the Work out of Hiring*, http://www.facebook.com/business/news/take-the-work-out-of-hiring (last visited Feb. 23, 2018).

[116] *See* 47 U.S.C. § 230(c)(2)(A) (2012) ("No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.").

the offending material.[117] This has been left to the courts to sort out. Distressed by the wide scope of the doctrine and some of these textual gaps, legislators and activists have been promoting amendments to Section 230 that would create exceptions for prostitution, nonconsensual pornography, and the sex trafficking of minors.[118] There is no reason why Congress couldn't also write in an explicit exception to Section 230 immunity for violations of civil rights laws.

Such proposals will face substantial pushback from intermediaries and others.[119] A company like Facebook, for example, has a lot to lose from any change that would require it to be more careful about how it distributes user content or generates personal or targeted advertisements.[120] Even a shift to what some are now calling "contextual advertising," where an advertiser buys the context in which social media users engage with each other rather than individual users' profiles, could cost a company like Facebook billions of dollars.[121] And to be sure, apart from the commercial interests at stake, there are important free speech arguments for keeping Section 230 broad: The content and data flowing through the online speech environment may not be as abundant in a world in which intermediaries are held to account for their users' content and their own designs on user data. But then again, it is difficult to weigh this "chilling" concern against the chilling of members of historically subordinated groups that is already happening under existing law.[122]

Whether legal reform in this area takes place in the legislature or the judiciary or both, reform is necessary. Judges, lawyers, and legislators should stop shielding intermediaries from liability on the basis of implausible assumptions about their neutrality or passivity—and should instead start looking carefully at how intermediaries' designs on user content do or do not result in actionable injuries. This attention to design will further sensitize intermediaries to the ways in which their services perpetuate systemic harms. Equipped with a more nuanced approach to intermediary immunity, we might come to expect an online environment that is hospitable to all comers.

---

[117] *Id.* § 230(f)(3). *See generally* Sylvain, *Design Duties*, *supra* note 21, at 239–42.

[118] *See* Stop Enabling Sex Traffickers Act of 2017, S. 1693, 115th Cong. (2017); Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong (2017).

[119] *See, e.g.*, Internet Ass'n, *Intermediary Liability*, http://internetassociation.org/positions/intermediary-liability (last visited Feb. 23, 2018); *see also* Electronic Frontier Found'n, *Stop SESTA: Congress Doesn't Understand How Section 230 Works* (Sept. 7, 2017), http://www.eff.org/deeplinks/2017/09/stop-sesta-congress-doesnt-understand-how-section-230-works.

[120] John Battelle, *Facebook Can't Be Fixed*, NewsCo (Jan. 5, 2018), http://shift.newco.co/its-the-advertising-model-stupid-b843cd7edbe9.

[121] *Id.*

[122] It is also difficult to disentangle this free speech argument from the intermediaries' commercial interests. European regulators, for instance, fined Google almost two and a half billion Euros last summer for abusing its market dominance in search to give "an illegal advantage to another Google product." European Commission, Press Release, *Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service* (June 27, 2017), http://europa.eu/rapid/press-release_IP-17-1784_en.htm.

Chapter 36

Toward a Clearer Conversation About Platform Liability (Daphne Keller)

Essays and Scholarship

Toward a Clearer Conversation About Platform Liability

Response to Olivier Sylvain's essay "Discriminatory Designs on User Data"

By Daphne Keller

https://knightcolumbia.org/content/toward-clearer-conversation-about-platform-liability

In his contribution to the Knight First Amendment Institute's "Emerging Threats" essay series, Fordham Law School's Olivier Sylvain critiques a core U.S. internet law, Section 230 of the Communications Decency Act (CDA 230).

CDA 230 immunizes platforms like YouTube and Craigslist from most liability for speech posted by their users. By doing so, it protects lawful and important speech that risk-averse platforms might otherwise silence. But it also lets platforms tolerate unlawful and harmful speech.

Sylvain argues that the net result is to perpetuate inequities in our society. For women, ethnic minorities, and many others, he suggests, CDA 230 facilitates harassment and abuse— and thus "helps to reinforce systemic subordination."

We need not tolerate all this harm, Sylvain further suggests, given the current state of technology. Large platforms' ever-improving ability to algorithmically curate users' speech "belies the old faith that such services operate at too massive a scale to be asked to police user content."

CDA 230 has long been a pillar of U.S. internet law. Lately, though, it has come under sustained attack. In the spring of 2018, Congress passed the first legislative change to CDA 230 in two decades: the Allow States and Victims to Fight Online Sex Trafficking Act, commonly known as FOSTA.

FOSTA has an important goal—protecting victims of sex trafficking. But it is so badly drafted, no one can agree on exactly what it means. It passed despite opposition from advocates for trafficking victims and the ACLU, and despite the Justice Department's concern that aspects of it could make prosecutors' jobs harder.

More challenges to CDA 230 are in the works. That makes close attention to the law, including both its strengths and its weaknesses, extremely timely.

Supporters of CDA 230 generally focus on three broad benefits. The first is promoting innovation and competition. When Congress passed the law in 1996, it was largely looking to future businesses and

technologies. In today's age of powerful mega-platforms, the concern about competition is perhaps even more justified. When platform liability risks expand, wealthy incumbents can hire lawyers and armies of moderators to adapt to new standards. Startups and smaller companies can't. That's why advocates for startups opposed FOSTA,

while Facebook and the incumbent-backed Internet Association supported it.

The second benefit of CDA 230 is its protection for internet users' speech rights. When platforms face liability for user content, they have strong incentives to err on the side of caution and take it down, particularly for controversial or unpopular material. Empirical evidence from notice-and-takedown regimes tells us that wrongful legal accusations are common, and that platforms often simply comply with them.

The Ecuadorian government, for example, has used spurious copyright claims to suppress criticism and videos of police brutality. Platform removal errors can harm any speaker, but a growing body of evidence suggests that they disproportionately harm vulnerable or disfavored groups.

So while Sylvain is right to say that vulnerable groups suffer disproportionately when platforms take down too little content, they also suffer disproportionately when platforms take down too much.

The third benefit is that CDA 230 encourages community-oriented platforms like Facebook or YouTube to weed out offensive content. This was Congress's goal in enacting the CDA's "Good Samaritan" clause, which immunizes platforms for voluntarily taking down anything they consider "objectionable."**14** Prior to CDA 230, platforms faced the so-called moderator's dilemma—any effort to weed out illegal content could expose them to liability for the things they missed, so they were safer not moderating at all.

Against these upsides, Sylvain marshals a compelling list of downsides. Permissive speech rules and hands-off attitudes by platforms, especially when combined with what Sylvain calls "discriminatory designs on user content and data," enable appalling abuses, particularly against members of minority groups. Nonconsensual pornography, verbal attacks, and credible threats of violence are all too common.

Does that mean it is time to scrap CDA 230? Some people think so. Sylvain's argument is more nuanced. He identifies specific harms, and specific advances in platform technology and operations, that he argues justify legal changes. While I disagree with some of his analysis and conclusions, the overall project is timely and useful. It arrives at a moment of chaotic, often rudderless public dialogue about platform responsibility. Pundits depict a maelstrom of online threats, often conflating issues as diverse as data breaches, "fake news," and competition. The result is a moment of real risk, not just for platforms but for internet users. Poorly thought-through policy responses to misunderstood problems can far too easily become laws.

In contrast to this panicked approach, Sylvain says we should be "looking carefully at how intermediaries' designs on user content do or do not result in actionable injuries." This is a worthy project. It is one that, in today's environment, requires us to pool our intellectual resources. Sylvain

brings, among other things, a deep understanding of the history of communications regulation. I bring practical experience from years in-house at Google and familiarity with intermediary liability laws around the world.

To put my own cards on the table—and surely surprising no one—I am very wary of tinkering with intermediary liability law, including CDA 230. That's mostly because I think the field is very poorly understood. It was hardly a field at all just a few years ago. A rising generation of experts, including Sylvain, will fix that before long. In the meantime, though, we need careful and calm analysis if we are to avoid shoot-from-the-hip legislative changes.

Whatever we do with the current slew of questions about platform responsibility, the starting point should be a close look at the facts and the law. The facts include the real and serious harms Sylvain identifies. He rightly asks why our system of laws tolerates them, and what we can do better.

CDA 230, though, is not the driver of many of the problems he identifies. In the first section of my response, I will walk through the reasons why. Hateful or harassing speech, for example, often doesn't violate any law at all for reasons grounded in the First Amendment. If platforms tolerate content of this sort, it is not because of CDA 230. Quite the contrary: A major function of the law is to *encourage* platforms to take down lawful but offensive speech.

Other problems Sylvain describes are more akin to the story, recently reported, of Facebook user data winding up in the hands of Cambridge Analytica.

They stem from breaches of trust (or of privacy or consumer protection law) between a platform and the user who shared data or content in the first place. Legal claims for breaching this trust are generally not immunized by CDA 230. If we want to change laws that apply in these situations, CDA 230 is the wrong place to start.

In the second section of my response, I will focus on the issues Sylvain surfaces that really do implicate CDA 230. In particular, I will discuss his argument that platforms' immunities should be reduced when they actively curate content and target it to particular users. Under existing intermediary liability frameworks outside of CDA 230, arguments for disqualifying platforms from immunity based on curation typically fall into one of two categories. I will address both.

The first argument is that platforms should not be immunized when they are insufficiently "neutral." This framing, I argue, is rarely helpful. It leads to confusing standards and in practice deters platforms from policing for harmful material.

The second argument is that immunity should depend on whether a platform "knows" about unlawful content. Knowledge is a slippery concept in the relevant law, but it is a relatively well-developed one. Knowledge-based liability has problems—it poses the very threats to speech, competition, and good-faith moderation efforts that CDA 230 avoids. But by talking about platform knowledge, we can reason from precedent and experience with other legal frameworks in the United States and around the world. That allows us to more clearly define the factual, legal, and policy questions in front of us. We can have

an intelligent conversation, even if we don't all agree. That's something the world of internet law and policy badly needs right now.

I. Isolating Non-CDA 230 Issues

In this section I will walk through issues and potential legal claims mentioned by Sylvain that are not, I think, controlled by CDA 230. Eliminating them from the discussion will help us focus on his remaining important questions about intermediary liability.

a. Targeting Content or Ads Based on Discriminatory Classifications

Sylvain's legal arguments are grounded in a deep moral concern with the harms of online discrimination. He provides numerous moving examples of bias and mistreatment. But many of the internet user and platform behaviors he describes are not actually illegal, or are governed by laws other than CDA 230.

As one particularly disturbing example, Sylvain describes how Facebook until recently allowed advertisers to target users based on algorithmically identified "interests" that included phrases like "how to burn Jews" and "Jew hater." When ProPublica's Julia Angwin broke this story, Facebook scrambled to suspend these interest categories. Sylvain recounts this episode to illustrate the kinds of antisocial outcomes that algorithmic decisionmaking can generate. However repugnant these phrases are, though, they are not illegal. Nor is using them to target ads. So CDA 230 does not increase platforms' willingness to tolerate this content—although it does increase their legal flexibility to take it down.

To outlaw this kind of thing, we would need different substantive laws about things like hate speech and harassment. Do we want those? Does the internet context change First Amendment analysis? Like other critics of CDA 230 doctrine, Sylvain emphasizes the "significant qualitative and quantitative difference between the reach of [harmful] offline and online expressive acts." But it's not clear that reforming CDA 230 alone would curb many of these harms in the absence of larger legal change.

CDA 230 also has little or no influence on Facebook ads that target users based on their likely race, age, or gender. Critics raise well-justified concerns about this targeting. But, as Sylvain notes, it generally is not illegal under current law. Anti-discrimination laws, and hence CDA 230 defenses, only come into play for ads regarding housing, employment, and possibly credit.

Even for that narrower class of ads, it's not clear that Facebook is doing anything illegal by offering a targeting tool that has both lawful and unlawful uses. If the Fair Housing Act (FHA) does apply to Facebook in this situation, the result in a CDA-230-less world would appear to be that Facebook must prohibit and remove these ads. But that's what Facebook says it does already.

So the CDA 230 problem here may be largely theoretical.

Sylvain's more complicated claim is that CDA 230 allows Airbnb to facilitate discrimination by requiring renters to post pictures of themselves. Given Airbnb's importance to travelers, discrimination

by hosts is a big deal. But CDA 230's relevance is dubious. First, it's not clear if anyone involved — even a host — violates the FHA by enforcing discriminatory preferences for shared dwellings.

Even if the hosts are liable, it seems unlikely that Airbnb violates the FHA by requiring photos, which serve legitimate as well as illegitimate purposes. Prohibiting the photos might even be unconstitutional: A court recently struck down under the First Amendment a California statute that, following reasoning similar to Sylvain's, barred the Internet Movie Database from showing actors' ages because employers might use the information to discriminate. Finally, if Airbnb's photo requirement did violate the FHA, it seems unlikely that CDA 230 would provide immunity.

The upshot is that CDA 230 is probably irrelevant to the problem Sylvain is trying to solve in this case.

None of this legal analysis refutes Sylvain's moral and technological point: The internet enables new forms of discrimination, and the law should respond. The law may very well warrant changing. But for these examples, CDA 230 isn't the problem.

b. Targeting Content Based on Data Mining

Sylvain also describes a set of problems that seem to arise from platforms' directly harming or breaching the trust of their users. Some of these commercial behaviors, like "administer[ing] their platforms in obscure or undisclosed ways that are meant to influence how users behave on the site," don't appear to implicate CDA 230 even superficially.

Others, like using user-generated content in ways the user did not expect, look more like CDA 230 issues because they involve publication. But I don't think they really fall under CDA 230 either.

In one particularly disturbing example, Sylvain describes an Instagram user who posted a picture of a rape threat she received—only to have Instagram reuse the picture as an ad. An analogous fact pattern was litigated under CDA 230 in *Fraley v. Facebook, Inc*.

In that case, users sued Facebook for using their profile pictures in ads, claiming a right-of-publicity violation. A court upheld their claim and rejected Facebook's CDA 230 defense.

If that ruling is correct, there should no CDA 230 issue for the case Sylvain describes.

But there is a deeper question about what substantive law governs in cases like this. The harm comes from a breach of trust between the platform and individual users, the kind of thing usually addressed by consumer protection, privacy, or data protection laws. U.S. law is famously weak in these areas. Compared to other countries, we give internet users few legal tools to control platforms' use of their data or content.

U.S. courts enforce privacy policies and terms of service that would be void in other jurisdictions, and they are stingy with standing or damages for people claiming privacy harms. That's why smart plaintiffs' lawyers bring claims like the right-of-publicity tort in *Fraley*. But the crux of those claims is not a publishing harm of the sort usually addressed by CDA 230. The crux is the user's lack of control over her *own* speech or data — what Jack Balkin or Jonathan Zittrain might call an "information fiduciary" issue.

Framing cases like these as CDA 230 issues risks losing sight of these other values and legal principles.

II. Addressing CDA 230 Issues

Sylvain suggests that platforms should lose CDA 230 immunity when they "employ software to make meaning out of their users' 'reactions,' search terms, and browsing activity in order to curate the content" and thereby "enable[] illegal online conduct." For issues that really do involve illegal content and potential liability for intermediaries—like nonconsensual pornography—this argument is important. At least one case has reviewed a nearly identical argument and rejected it.

But Sylvain's point isn't to clarify the current law. It's to work toward what he calls "a more nuanced immunity doctrine." For that project, the curation argument matters.

I see two potential reasons for stripping platforms of immunity when they "elicit and then algorithmically sort and repurpose" user content.

First, a platform might lose immunity because it is not "neutral" enough, given the ways it selects and prioritizes particular material.

Second, it could lose immunity because curation efforts give it "knowledge" of unlawful material. Both theories have important analogues in other areas of law—including the Digital Millennium Copyright Act (DMCA), pre-CDA U.S. law, and law from outside the United States—to help us think them through.

a. Neutrality

All intermediary liability laws have some limit on the platform operations that are immunized—a point at which a platform becomes too engaged in user-generated content and starts being held legally responsible for it. Courts and lawmakers often use words like "neutral" or "passive" to describe immunized platforms. Those words don't, in my experience, have stable enough meanings to be useful.

For example, the Court of Justice of the European Union has said that only "passive" hosts are immune under EU law. Applying that standard in the leading case, it found Google immune for content in ads, which the company not only organizes and ranks but also ranks based in part on payment.

And in a U.S. case, a court said a platform was "neutral" when it engaged in the very kinds of curation that, under Sylvain's analysis, makes platforms *not* neutral.

In the internet service provider (ISP) context, neutrality—as in net neutrality—means something very different. Holding ISPs to a "passive conduit" standard makes sense as a technological matter. But that standard doesn't transfer well to other intermediaries. It would eliminate immunity for topic-specific forums (Disney's Club Penguin or a subreddit about knitting, for example) or for platforms like Facebook that bar lawful but offensive speech. That seems like the wrong outcome given that most users, seemingly including Sylvain, *want* platforms to remove this content.

Policymakers could in theory draw a line by saying that, definitionally, a platform that algorithmically curates content is not neutral or immunized. But then what do we do with search engines, which offer algorithmic ranking as their entire value proposition? And how exactly does a no-algorithmic-curation

standard apply to social media? As Eric Goldman has pointed out, there is no such thing neutrality for a platform, like Facebook or Twitter, that hosts user-facing content.

Whether it sorts content chronologically, alphabetically, by size, or some other metric, it unavoidably imposes a hierarchy of some sort.

All of this makes neutrality something of a Rorschach test. It takes on different meanings depending on the values we prioritize. For someone focused on speech rights, neutrality might mean not excluding any legal content, no matter how offensive. For a competition specialist, it might mean honesty and fair competition in ranking search results.

Still other concepts of neutrality might emerge if we prioritize competition, copyright, transparency, or, as Sylvain does in this piece, protecting vulnerable groups in society.

One way out of this bind is for the law to get very, very granular—like the DMCA. It has multiple overlapping statutory tests that effectively assess a defendant's neutrality before awarding immunity.

By focusing on just a few values, narrowly defining eligible technologies, and spelling out rules in detail, it's easier to define the line between immunized behavior and non-immunized behavior.

DMCA litigators on both sides hate these granular tests. Maybe that means the law is working as intended. But highly particular tests for immunity present serious tradeoffs. If every intermediary liability question looked like the DMCA, then only companies with armies of lawyers and reserves of cash for litigation and settlement could run platforms. And even they would block user speech or decide not to launch innovative features in the face of legal uncertainty. Detailed rules like the DMCA's get us back to the problems that motivated Congress to pass the CDA: harm to lawful speech, harm to competition and innovation, and uncertainty about whether platforms could moderate content without incurring liability.

Congress's goal in CDA 230 was to get away from neutrality tests as a basis for immunity and instead to encourage platforms to curate content. I think Congress was right on this score, and not only for the competition, speech, and "Good Samaritan" reasons identified at the time. As Sylvain's discussion of intermediary designs suggests, abstract concepts of neutrality do not provide workable answers to real-world platform liability questions.

b. Knowledge

The other interpretation I see for Sylvain's argument about curation is that platforms shouldn't be able to claim immunity if they know about illegal content—and that the tools used for curation bring them ever closer to such knowledge. This factual claim is debatable. Do curation, ranking, and targeting algorithms really provide platforms with meaningful information about legal violations?

Whatever the answer, focusing on questions like this can clarify intermediary liability discussions.

Like the neutrality framing, this one is familiar from non-CDA 230 intermediary liability. Many laws around the world, including parts of the DMCA, say that if a platform knows about unlawful content but doesn't take it down, it loses immunity. These laws lead to litigation about what counts as

"knowledge," and to academic, NGO, and judicial attention to the effects on the internet ecosystem. If a mere allegation or notice to a platform creates culpable knowledge, platforms will err on the side of removing lawful speech. If "knowledge" is an effectively unobtainable legal ideal, on the other hand, platforms won't have to take down anything.

Some courts and legislatures around the world have addressed this problem by reference to due process. Platforms in Brazil,

Chile, Spain, India, and Argentina are, for some or all claims, not considered to know whether a user's speech is illegal until a court has made that determination. Laws like these often make exceptions for "manifestly" unlawful content that can, in principle, be identified by platforms. This is functionally somewhat similar to CDA 230's exception for child pornography and other content barred by federal criminal law.

Other models, like the DMCA, use procedural rules to cabin culpable knowledge. Sylvain rightly invokes these as important protections against abuse of notice-and-takedown systems. Claimants must follow a statutorily defined notice process and provide a penalty-of-perjury statement. A DMCA notice that does not comply with the statute's requirements cannot be used to prove that a platform knows about infringing material.

Claimants also accept procedures for accused speakers to formally challenge a removal or to seek penalties for bad-faith removal demands.

A rapidly expanding body of material from the United Nations and regional human rights systems,

as well as a widely endorsed civil society standard known as the Manila Principles, spell out additional procedures designed to limit over-removal of lawful speech. Importantly, these include public transparency to allow NGOs and internet users to crowdsource the job of identifying errors by platforms and patterns of abuse by claimants. Several courts around the world have also cited constitutional free expression rights of internet users in rejecting—as Sylvain does—strict liability for platforms.

As Sylvain notes, liability based on knowledge is common in pre-CDA tort law. Platforms differ from print publishers and distributors in important respects. But case law about "analog intermediaries" can provide important guidance, some of it mandatory under the First Amendment. The "actual malice" standard established in *New York Times Co. v. Sullivan* is an example.

Importantly, the *Times* in that case acted as a platform, not as a publisher of its own reporting. The speech at issue came from paying advertisers, who bought space in the paper to document violence against civil rights protesters. As the court noted in rejecting the Alabama Supreme Court's defamation judgment, high liability risk "would discourage newspapers from carrying 'editorial advertisements' of this type, and so might shut off an important outlet for the promulgation of information and ideas by persons who do not themselves have access to publishing facilities."

Similar considerations apply online.

Knowledge-based standards for platform liability are no panacea.

Any concept of culpable knowledge for speech platforms involves tradeoffs of competing values, and not ones I necessarily believe we should make. What the knowledge framing and precedent provide, though, is a set of tools for deliberating more clearly about those tradeoffs.

III. Conclusion

Talk of platform regulation is in the air. Lawyers can make sense of this chaotic public dialogue by being lawyerly. We can crisply identify harms and parse existing laws. If those laws aren't adequately protecting important values, including the equality values Sylvain discusses, we can propose specific changes and consider their likely consequences.

At the end of the day, not everyone will agree about policy tradeoffs in intermediary liability—how to balance speech values against dignity and equality values, for example. And not everyone will have the same empirical predictions about what consequences laws are likely to have. But we can get a whole lot closer to agreement than we are now. We can build better shared language and analytic tools, and identify the right questions to ask. Sylvain's observations and arguments, coupled with tools from existing intermediary liability law, can help us do that.

Note: The author was formerly Associate General Counsel to Google. The Center for Internet and Society (CIS) is a public interest technology law and policy program at Stanford Law School. A list of CIS donors and funding policies is available here.

Daphne Keller is the Director of Intermediary Liability at the Stanford Center for Internet and Society.

Chapter 37

A Human Rights Approach to Platform Content Regulation (David Kaye)

United Nations A/HRC/38/35

General Assembly

Distr.: General
6 April 2018

Original: English

Human Rights Council
Thirty-eighth session
18 June–6 July 2018
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Note by the Secretariat

The Secretariat has the honour to transmit to the Human Rights Council the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, pursuant to Council resolution 34/18. In his report the Special Rapporteur addresses the regulation of user-generated online content. He recommends that States ensure an enabling environment for online freedom of expression and that companies apply human rights standards at all stages of their operations. Human rights law gives companies the tools to articulate their positions in ways that respect democratic norms and counter authoritarian demands. At a minimum, companies and States should pursue radically improved transparency, from rule-making to enforcement of the rules, to ensure user autonomy as individuals increasingly exercise fundamental rights online.

GE.18-05436(E)
1805436

A/HRC/38/35

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Contents

I. Introduction

1. Early in the digital age, John Perry Barlow declared that the Internet would usher in "a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity".[1] Although the Internet remains history's greatest tool for global access to information, such online evangelism is hard to find today. The public sees hate, abuse and disinformation in the content users generate. Governments see terrorist recruitment or discomfiting dissent and opposition. Civil society organizations see the outsourcing of public functions, like protection of freedom of expression, to unaccountable private actors. Despite taking steps to illuminate their rules and government interactions, the companies remain enigmatic regulators, establishing a kind of "platform law" in which clarity, consistency, accountability and remedy are elusive. The United Nations, regional organizations and treaty bodies have affirmed that offline rights apply equally online, but it is not always clear that the companies protect the rights of their users or that States give companies legal incentives to do so.

2. In the present report the Special Rapporteur proposes a framework for the moderation of user-generated online content that puts human rights at the very centre.[2] He seeks to answer basic questions: What responsibilities do companies have to ensure that their platforms do not interfere with rights guaranteed under international law? What standards should they apply to content moderation? Should States regulate commercial content moderation and, if so, how? The law expects transparency and accountability from States to mitigate threats to freedom of expression. Should we expect the same of private actors? What do the processes of protection and remedy look like in the digital age?

3. Previous reports have addressed some of these questions.[3] The present report focuses on the regulation of user-generated content, principally by States and social media companies but in a way that is applicable to all relevant actors in the information and communications technology (ICT) sector. The Special Rapporteur outlines the applicable human rights legal framework and describes company and State approaches to content regulation. He proposes standards and processes that companies should adopt to regulate content in accordance with human rights law.

4. Research into the companies' terms of service, transparency reporting and secondary sources provided the initial basis for the report. Calls for comments generated 21 submissions from States and 29 from non-State actors (including 1 company submission). The Special Rapporteur visited several companies in Silicon Valley and held conversations with others in an effort to understand their approaches to content moderation.[4] He benefited from civil society consultations held in Bangkok and Geneva in 2017 and 2018 and online discussions with experts in Latin America, the Middle East and North Africa and sub-Saharan Africa in 2018.[5]

II. Legal framework

5. The activities of companies in the ICT sector implicate rights to privacy, religious freedom and belief, opinion and expression, assembly and association, and public participation, among others. The present report focuses on freedom of expression while

[1] John Perry Barlow, A Declaration of the Independence of Cyberspace, 8 February 1996.

[2] "Moderation" describes the process by which Internet companies determine whether user-generated content meets the standards articulated in their terms of service and other rules.

[3] A/HRC/35/22 and A/HRC/32/38.

[4] The Special Rapporteur visited the headquarters of Facebook, Github, Google, Reddit and Twitter and held conversations with representatives of Yahoo/Oath, Line and Microsoft. He also visited the non-profit Wikimedia Foundation. He hopes to visit companies in Beijing, Moscow, Seoul and Tokyo in work related to the present report.

[5] The Special Rapporteur wishes to thank his legal adviser, Amos Toh, and students at the International Justice Clinic at the University of California, Irvine, School of Law.

acknowledging the interdependence of rights, such as the importance of privacy as a gateway to freedom of expression.[6] Article 19 of the International Covenant on Civil and Political Rights provides globally established rules, ratified by 170 States and echoing the Universal Declaration of Human Rights, guaranteeing "the right to hold opinions without interference" and "the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers" and through any medium.[7]

A. State obligations

6. Human rights law imposes duties on States to ensure enabling environments for freedom of expression and to protect its exercise. The duty to ensure freedom of expression obligates States to promote, *inter alia*, media diversity and independence and access to information.[8] Additionally, international and regional bodies have urged States to promote universal Internet access.[9] States also have a duty to ensure that private entities do not interfere with the freedoms of opinion and expression.[10] The Guiding Principles on Business and Human Rights, adopted by the Human Rights Council in 2011, emphasize in principle 3 State duties to ensure environments that enable business respect for human rights.[11]

7. States may not restrict the right to hold opinions without interference. Per article 19 (3) of the Covenant, State limitations on freedom of expression must meet the following well-established conditions:

- *Legality*. Restrictions must be "provided by law". In particular, they must be adopted by regular legal processes and limit government discretion in a manner that distinguishes between lawful and unlawful expression with "sufficient precision". Secretly adopted restrictions fail this fundamental requirement.[12] The assurance of legality should generally involve the oversight of independent judicial authorities.[13]
- *Necessity and proportionality*. States must demonstrate that the restriction imposes the least burden on the exercise of the right and actually protects, or is likely to protect, the legitimate State interest at issue. States may not merely assert necessity but must demonstrate it, in the adoption of restrictive legislation and the restriction of specific expression.[14]
- *Legitimacy*. Any restriction, to be lawful, must protect only those interests enumerated in article 19 (3): the rights or reputations of others, national security or public order, or public health or morals. Restrictions designed to protect the rights of others, for instance, include "human rights as recognized in the Covenant and more generally in international human rights law".[15] Restrictions to protect rights to privacy, life, due process, association and participation in public affairs, to name a few, would be legitimate when demonstrated to meet the tests of legality and necessity. The Human Rights Committee cautions that restrictions to protect "public

[6] See A/HRC/29/32, paras. 16–18.

[7] See also African Charter on Human and Peoples' Rights, art. 9; American Convention on Human Rights, art. 13; Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10. See also Centro de Estudios en Libertad de Expresión y Acceso a la Información submission.

[8] Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, 3 March 2017, sect. 3. See also Human Rights Committee, general comment No. 34 (2011) on the freedoms of opinion and expression, paras. 18 and 40; A/HRC/29/32, para. 61 and A/HRC/32/38, para. 86.

[9] See Human Rights Council, resolution 32/13, para. 12; Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, *Standards for a Free, Open and Inclusive Internet* (2016), para. 18.

[10] See general comment No. 34, para. 7.

[11] A/HRC/17/31.

[12] Ibid. para. 25; A/HRC/29/32.

[13] Ibid.

[14] See general comment No. 34, para. 27.

[15] Ibid., para. 28.

morals" should not derive "exclusively from a single tradition", seeking to ensure that the restriction reflects principles of non-discrimination and the universality of rights.[16]

8. Restrictions pursuant to article 20 (2) of the Covenant — which requires States to prohibit "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence" — must still satisfy the cumulative conditions of legality, necessity and legitimacy.[17]

B. Company responsibilities

9. Internet companies have become central platforms for discussion and debate, information access, commerce and human development.[18] They collect and retain the personal data of billions of individuals, including information about their habits, whereabouts and activities, and often claim civic roles. In 2004, Google promoted its ambition to do "good things for the world even if we forgo some short term gains".[19] Facebook's founder has proclaimed a desire to "develop the social infrastructure to give people the power to build a global community that works for all of us".[20] Twitter has promised policies that "improve — and do not detract from — a free and global conversation".[21] VKontakte, a Russian social media company, "unites people all over the world", while Tencent reflects the language of the Government of China when noting its aims to "help build a harmonious society and to become a good corporate citizen".[22]

10. Few companies apply human rights principles in their operations, and most that do see them as limited to how they respond to government threats and demands.[23] However, the Guiding Principles on Business and Human Rights establish "global standard[s] of expected conduct" that should apply throughout company operations and wherever they operate.[24] While the Guiding Principles are non-binding, the companies' overwhelming role in public life globally argues strongly for their adoption and implementation.

11. The Guiding Principles establish a framework according to which companies should, at a minimum:

(a) Avoid causing or contributing to adverse human rights impacts and seek to prevent or mitigate such impacts directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts (principle 13);

(b) Make high-level policy commitments to respect the human rights of their users (principle 16);

(c) Conduct due diligence that identifies, addresses and accounts for actual and potential human rights impacts of their activities, including through regular risk and impact assessments, meaningful consultation with potentially affected groups and other stakeholders, and appropriate follow-up action that mitigates or prevents these impacts (principles 17−19);

(d) Engage in prevention and mitigation strategies that respect principles of internationally recognized human rights to the greatest extent possible when faced with conflicting local law requirements (principle 23);

[16] Ibid., para. 32.
[17] Ibid., para. 50. See also A/67/357.
[18] See, for example, Supreme Court of the United States, *Packingham v. North Carolina*, opinion of 19 June 2017; European Court of Human Rights, *Times Newspapers Ltd. (Nos. 1 and 2) v. The United Kingdom* (application Nos. 3002/03 and 23676/03), judgment of 10 March 2009, para. 27.
[19] Securities Registration Statement (S-1) under the Securities Act of 1933, 18 August 2004.
[20] Mark Zuckerberg, "Building global community", Facebook, 16 February 2017.
[21] Twitter, S-1 Registration Statement, 13 October 2013, pp. 91–92.
[22] VKontakte, company information; Tencent, "About Tencent".
[23] Danish Institute for Human Rights submission. Cf. Yahoo/Oath submission, 2016.
[24] Guiding Principles, principle 11.

(e) Conduct ongoing review of their efforts to respect rights, including through regular consultation with stakeholders, and frequent, accessible and effective communication with affected groups and the public (principles 20−21);

(f) Provide appropriate remediation, including through operational-level grievance mechanisms that users may access without aggravating their "sense of disempowerment" (principles 22, 29 and 31).

III. Key concerns with content regulation

12. Governments seek to shape the environment in which companies moderate content, while the companies predicate individual access to their platforms on user agreement with terms of service that govern what may be expressed and how individuals may express it.

A. Government regulation

13. States regularly require companies to restrict manifestly illegal content such as representations of child sexual abuse, direct and credible threats of harm and incitement to violence, presuming they also meet the conditions of legality and necessity.[25] Some States go much further and rely on censorship and criminalization to shape the online regulatory environment.[26] Broadly worded restrictive laws on "extremism", blasphemy, defamation, "offensive" speech, "false news" and "propaganda" often serve as pretexts for demanding that companies suppress legitimate discourse.[27] Increasingly, States target content specifically on online platforms.[28] Other laws may interfere with online privacy in ways that deter the exercise of freedom of opinion and expression.[29] Many States also deploy tools of disinformation and propaganda to limit the accessibility and trustworthiness of independent media.[30]

14. *Liability protections*. From early in the digital age, many States adopted rules to protect intermediaries from liability for the content third parties publish on their platforms. The European Union e-commerce directive, for instance, establishes a legal regime to protect intermediaries from liability for content except when they go beyond their role as a "mere conduit", "cache" or "host" of information provided by users.[31] Section 230 of the United States Communications Decency Act generally provides immunity for providers of "interactive computer service[s]" that host or publish information about others, but this has since been curtailed.[32] The intermediary liability regime in Brazil requires a court order to restrict particular content,[33] while the intermediary liability regime in India establishes a "notice and takedown" process that involves the order of a court or similar adjudicative

[25] Ireland has established co-regulatory mechanisms with companies to restrict illegal child sexual abuse material: Ireland submission. Many companies rely on a picture recognition algorithm to detect and remove child pornography: submissions by Open Technology Institute, p. 2 and ARTICLE 19, p. 8.

[26] See A/HRC/32/38, paras. 46−47. On Internet shutdowns, see A/HRC/35/22, paras. 8−16 and examples of communications of the Special Rapporteur: Nos. UA TGO 1/2017, UA IND 7/2017 and AL GMB 1/2017.

[27] Communication Nos. OL MYS 1/2018; UA RUS 7/2017; UA ARE 7/2017, AL BHR 8/2016, AL SGP 5/2016 and OL RUS 7/2016. Azerbaijan prohibits propaganda of terrorism, religious extremism and suicide: Azerbaijan submission.

[28] See communication Nos. OL PAK 8/2016 and OL LAO 1/2014; Association for Progressive Communications, *Unshackling Expression: A Study on Laws Criminalising Expression Online in Asia*, GISWatch 2017 Special Edition.

[29] A/HRC/29/32.

[30] See, for example, Gary King, Jennifer Pan and Margaret E. Roberts, "How the Chinese Government fabricates social media posts for strategic distraction, not engaged argument", *American Political Science Review*, vol. 111, No. 3 (2017), pp. 484−501.

[31] Directive No. 2000/31/EC of the European Parliament and of the Council of 8 June 2000.

[32] 47 United States Code § 230. See also the Allow States and Victims to Fight Online Sex Trafficking Act (H.R. 1865).

[33] *Marco Civil da Internet*, federal law 12.965, arts. 18−19.

body.[34] The 2014 Manila Principles on Intermediary Liability, developed by a coalition of civil society experts, identify essential principles that should guide any intermediary liability framework.

15. *Imposition of company obligations*. Some States impose obligations on companies to restrict content under vague or complex legal criteria without prior judicial review and with the threat of harsh penalties. For example, the Chinese Cybersecurity Law of 2016 reinforces vague prohibitions against the spread of "false" information that disrupts "social or economic order", national unity or national security; it also requires companies to monitor their networks and report violations to the authorities.[35] Failure to comply has reportedly led to heavy fines for the country's biggest social media platforms.[36]

16. Obligations to monitor and rapidly remove user-generated content have also increased globally, establishing punitive frameworks likely to undermine freedom of expression even in democratic societies. The network enforcement law (*NetzDG*) in Germany requires large social media companies to remove content inconsistent with specified local laws, with substantial penalties for non-compliance within very short time frames.[37] The European Commission has even recommended that member States establish legal obligations for active monitoring and filtering of illegal content.[38] Guidelines adopted in 2017 in Kenya on the dissemination of social media content during elections require platforms to "pull down accounts used in disseminating undesirable political contents on their platforms" within 24 hours.[39]

17. In the light of legitimate State concerns such as privacy and national security, the appeal of regulation is understandable. However, such rules involve risks to freedom of expression, putting significant pressure on companies such that they may remove lawful content in a broad effort to avoid liability. They also involve the delegation of regulatory functions to private actors that lack basic tools of accountability. Demands for quick, automatic removals risk new forms of prior restraint that already threaten creative endeavours in the context of copyright.[40] Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic.[41]

18. *Global removals*. Some States are demanding extraterritorial removal of links, websites and other content alleged to violate local law.[42] Such demands raise serious

[34] Supreme Court of India, *Shreya Singhal v. Union of India*, decision of 24 March 2015.

[35] Articles 12 and 47; Human Rights in China submission, 2016, p. 12. For comments on an earlier draft of the Cybersecurity Law, see communication No. OL CHN 7/2015. See also Global Voices, "Netizen Report: Internet censorship bill looms large over Egypt", 16 March 2018; Republic of South Africa, Films and Publications Amendment Bill (B 61—2003).

[36] PEN America, *Forbidden Feeds: Government Controls on Social Media in China* (2018), p. 21.

[37] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), July 2017. See communication No. OL DEU 1/2017.

[38] European Commission, recommendation on measures to effectively tackle illegal content online (last updated: 5 March 2018).

[39] See communication No. OL KEN 10/2017; Javier Pallero, "Honduras: new bill threatens to curb online speech", Access Now, 12 February 2018.

[40] See European Commission, Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, COM (2016) 593 final, art. 13; Daphne Keller, "Problems with filters in the European Commission's platforms proposal", Stanford Law School Center for Internet and Society, 5 October 2017; Fundación Karisma submission, 2016, pp. 4–6.

[41] Under European Union law, search engines are required to determine the validity of claims brought under the "right to be forgotten" framework. European Court of Justice, *Google Spain v. Agencia Española de Protección de Datos and Mario Costeja González* (case C-131/12), judgment (Grand Chamber) of 13 May 2014; submissions by ARTICLE 19, pp. 2–3 and Access Now, pp. 6–7; Google, "Updating our 'right to be forgotten' Transparency Report"; Theo. Bertram and others, *Three Years of the Right to be Forgotten* (Google, 2018).

[42] See, for example, PEN America, *Forbidden Feeds*, pp. 36–37; Supreme Court of Canada, *Google Inc. v. Equestek Solutions Inc*., judgment of 28 June 2017; European Court of Justice, *Google Inc. v.*

concern that States may interfere with the right to freedom of expression "regardless of frontiers". The logic of these demands would allow censorship across borders, to the benefit of the most restrictive censors. Those seeking removals should be required to make such requests in every jurisdiction where relevant, through regular legal and judicial process.

19. *Government demands not based on national law*. Companies distinguish between requests for the removal of allegedly illegal content submitted through regular legal channels and requests for removal based on the companies' terms of service.[43] (Legal removals generally apply only in the requesting jurisdiction; terms of service removals generally apply globally.) State authorities increasingly seek content removals outside of legal process or even through terms of service requests.[44] Several have established specialized government units to refer content to companies for removal. The European Union Internet Referral Unit, for instance, "flag[s] terrorist and violent extremist content online and cooperat[es] with online service providers with the aim of removing this content".[45] Australia also has similar referral mechanisms.[46] In South-East Asia, parties allied with Governments reportedly attempt to use terms of service requests to restrict political criticism.[47]

20. States also place pressure on companies to accelerate content removals through non-binding efforts, most of which have limited transparency. A three-year ban on YouTube in Pakistan compelled Google to establish a local version susceptible to government demands for removals of "offensive" content.[48] Facebook and Israel reportedly agreed to coordinate efforts and staff to monitor and remove "incitement" online. The details of this agreement were not disclosed, but the Israeli Minister of Justice claimed that between June and September 2016, Facebook granted nearly all government requests for removal of "incitement".[49] Arrangements to coordinate content actions with State input exacerbate concerns that companies perform public functions without the oversight of courts and other accountability mechanisms.[50]

21. The 2016 European Union Code of Conduct on countering illegal hate speech online involves agreement between the European Union and four major companies to remove content, committing them to collaborate with "trusted flaggers" and promote "independent counter-narratives".[51] While the promotion of counter-narratives may be attractive in the face of "extremist" or "terrorist" content, pressure for such approaches runs the risk of transforming platforms into carriers of propaganda well beyond established areas of legitimate concern.[52]

Commission nationale de l'informatique et des libertés (CNIL) (case C-507/17); Global Network Initiative submission, p. 6.

[43] Compare Twitter Transparency Report: Removal Requests (January−June 2017) with Twitter Transparency Report: Government Terms of Service Reports (January−June 2017). See also Facebook, Government requests: Frequently Asked Questions (FAQs).

[44] Submissions by ARTICLE 19, p. 2 and Global Network Initiative, p. 5.

[45] European Union, Internet Referral Unit, Year One Report, sect. 4.11; submissions by European Digital Rights (EDRi), p. 1 and Access Now, pp. 2−3.

[46] Australia submission.

[47] Southeast Asian Press Alliance, p. 1.

[48] Digital Rights Foundation submission.

[49] 7amleh − The Arab Center for the Advancement of Social Media submission.

[50] Association for Progressive Communications, p. 14 and 7amleh.

[51] "Trusted flaggers … refers to the status given to certain organisations which allows them to report illegal content through a special reporting system or channel, which is not available to normal users." European Commission, Code of Conduct on countering illegal hate speech online: First results on implementation (December 2016).

[52] The same companies created the Global Internet Forum to Counter Terrorism, an effort to develop industry-wide technological tools to remove terrorist content on their platforms. Google, "Update on the Global Internet Forum to Counter Terrorism", 4 December 2017.

B. Company moderation of content

Company compliance with national law

22. Each company is committed in principle to comply with the local law where it does business. As Facebook puts it: "If, after careful legal review, we determine that the content is illegal under local law, then we make it unavailable in the relevant country or territory."[53] Tencent, the owner of the mobile chat and social media app WeChat, goes considerably further, requiring anyone using the platform within China and Chinese citizens using the platform "anywhere in the world" to comply with content restrictions that mirror Chinese law or policy.[54] Several companies also collaborate with one another and regulatory bodies to remove images of child sexual abuse.[55]

23. The commitment to legal compliance can be complicated when relevant State law is vague, subject to varying interpretations or inconsistent with human rights law. For instance, laws against "extremism" which leave the key term undefined provide discretion to government authorities to pressure companies to remove content on questionable grounds.[56] Similarly, companies are often under pressure to comply with State laws that criminalize content that is said to be, for instance, blasphemous, critical of the State, defamatory of public officials or false. As explained below, the Guiding Principles provide tools to minimize the impact of such laws on individual users. The Global Network Initiative, a multi-stakeholder initiative that helps ICT companies navigate human rights challenges, has developed additional guidance on how to employ these tools.[57] One tool of minimization is transparency: many companies report annually on the number of government requests they receive and execute per State.[58] However, companies do not consistently disclose sufficient information about how they respond to government requests, nor do they regularly report government requests made under terms of service.[59]

Company moderation standards

24. Internet companies require their users to abide by terms of service and "community standards" that govern expression on their platforms.[60] Company terms of service, which users are required to accept in exchange for use of the platform, identify jurisdictions for dispute resolution and reserve to themselves discretion over content and account actions.[61] Platform content policies are a subset of these terms, articulating constraints on what users may express and how they may express it. Most companies do not explicitly base content

[53] Facebook, Government requests: FAQs. See also Google legal removal requests; Twitter rules and policies; Reddit content policy.

[54] Tencent, Terms of Service: Introduction; Tencent, Agreement on Software License and Service of Tencent Wenxin.

[55] United Nations Educational, Scientific and Cultural Organization, *Fostering Freedom Online: The Role of Internet Intermediaries* (Paris, 2014), pp. 56−57.

[56] See Maria Kravchenko, "Inappropriate enforcement of anti-extremist legislation in Russia in 2016", SOVA Center for Information and Analysis, 21 April 2017; Danielle Citron, "Extremist speech, compelled conformity, and censorship creep", *Notre Dame Law Review*, vol. 93, No. 3 (2018), pp. 1035−1071.

[57] Global Network Initiative, Principles on Freedom of Expression and Privacy, sect. 2. Social media companies participating in the Initiative include Facebook, Google, Microsoft/LinkedIn and Yahoo/Oath.

[58] See paragraph 39 below. In addition, Automattic, Google, Microsoft/Bing and Twitter are among the companies that regularly, although not necessarily comprehensively, post government takedown and intellectual property requests to the Lumen database.

[59] Ranking Digital Rights, 2017 Corporate Accountability Index, p. 28.

[60] Jamila Venturini and others, *Terms of Service and Human Rights: An Analysis of Online Platform Contracts* (Rio de Janeiro, Revan, 2016).

[61] Baidu user agreement ("[We] remove and delete any content in this service based on Baidu's own discretion for any reason."); Tencent terms of service ("We reserve the right to block or remove Your Content for any reason, including as is in our opinion appropriate or as required by applicable laws and regulations."); Twitter terms of service ("We may suspend or terminate your account or cease providing you with all or part of the Services at any time for any or no reason.").

standards on any particular body of law that might govern expression, such as national law or international human rights law. The Chinese search giant Baidu, however, prohibits content that is "opposed to the basic principles established by the Constitution" of the People's Republic of China.[62]

25. The development of content moderation policies typically involves legal counsel, public policy and product managers, and senior executives. Companies may establish "trust and safety" teams to address spam, fraud and abuse, and counter-terrorism teams may address terrorist content.[63] Some have developed mechanisms for soliciting input from outside groups on specialized aspects of content policies.[64] The exponential increase in user-generated content has triggered the development of detailed and constantly evolving rules. These rules vary according to a range of factors, from company size, revenue and business model to the "platform's brand and reputation, its tolerance for risk, and the type of user engagement it wishes to attract".[65]

Areas of concern around content standards

26. *Vague rules*. Company prohibitions of threatening or promoting terrorism,[66] supporting or praising leaders of dangerous organizations[67] and content that promotes terrorist acts or incites violence[68] are, like counter-terrorism legislation, excessively vague.[69] Company policies on hate, harassment and abuse also do not clearly indicate what constitutes an offence. Twitter's prohibition of "behavior that incites fear about a protected group" and Facebook's distinction between "direct attacks" on protected characteristics and merely "distasteful or offensive content" are subjective and unstable bases for content moderation.[70]

27. *Hate, harassment, abuse*. The vagueness of hate speech and harassment policies has triggered complaints of inconsistent policy enforcement that penalizes minorities while reinforcing the status of dominant or powerful groups. Users and civil society report violence and abuse against women, including physical threats, misogynist comments, the posting of non-consensual or fake intimate images and doxing;[71] threats of harm against the politically disenfranchised,[72] minority races and castes[73] and ethnic groups suffering from violent persecution;[74] and abuse directed at refugees, migrants and asylum seekers.[75] At the same time, platforms have reportedly suppressed lesbian, gay, bisexual, transgender and queer activism,[76] advocacy against repressive Governments,[77] reporting on ethnic cleansing[78] and critiques of racist phenomena and power structures.[79]

[62] Baidu terms of service, sect. 3.1.
[63] Monika Bickert, "Hard questions: how we counter terrorism", 15 June 2017.
[64] See, for example, Twitter Trust and Safety Council and YouTube Trusted Flagger Program.
[65] Sarah Roberts, *Content Moderation* (University of California at Los Angeles, 2017). See also ARTICLE 19 submission, p. 2.
[66] Twitter rules and policies (violent extremist groups).
[67] Facebook community standards (dangerous organizations).
[68] YouTube policies (violent or graphic content policies).
[69] See A/HRC/31/65, para. 39.
[70] Facebook community standards (hate speech); Twitter rules and policies (hateful conduct policy).
[71] Amnesty International, *Toxic Twitter: A Toxic Place for Women*; Association for Progressive Communications submission, p. 2.
[72] Submissions by 7amleh and Association for Progressive Communications, p. 15.
[73] Ijeoma Oluo, "Facebook's complicity in the silencing of black women", Medium, 2 August 2017; submissions by Center for Communications Governance, p. 5 and Association for Progressive Communications, pp. 11−12.
[74] Statement by the Special Rapporteur on the situation of human rights in Myanmar, Yanghee Lee, to the thirty-seventh session of the Human Rights Council, 12 March 2018.
[75] Association for Progressive Communications submission, p. 12.
[76] Electronic Frontier Foundation submission, p. 5.
[77] Ibid.; submissions by Association for Progressive Communications and 7amleh.
[78] Betsy Woodruff, "Facebook silences Rohingya reports of ethnic cleansing", The Daily Beast, 18 September 2017; ARTICLE 19 submission, p. 9.

28. The scale and complexity of addressing hateful expression presents long-term challenges and may lead companies to restrict such expression even if it is not clearly linked to adverse outcomes (as hateful advocacy is connected to incitement in article 20 of the International Covenant on Civil and Political Rights). Companies should articulate the bases for such restrictions, however, and demonstrate the necessity and proportionality of any content actions (such as removals or account suspensions). Meaningful and consistent transparency about enforcement of hate speech policies, through substantial reporting of specific cases, may also provide a level of insight that even the most detailed explanations cannot offer.[80]

29. *Context*. Companies emphasize the importance of context when assessing the applicability of general restrictions.[81] Nonetheless, attention to context has not prevented removals of depictions of nudity with historical, cultural or educational value;[82] historical and documentary accounts of conflict;[83] evidence of war crimes;[84] counter speech against hate groups;[85] or efforts to challenge or reclaim racist, homophobic or xenophobic language.[86] Meaningful examination of context may be thwarted by time and resource constraints on human moderators, overdependence on automation or insufficient understanding of linguistic and cultural nuance.[87] Companies have urged users to supplement controversial content with contextual details, but the feasibility and effectiveness of this guidance are unclear.[88]

30. *Real-name requirements*. In order to deal with online abuse, some companies have "authentic identity" requirements;[89] others approach identity questions more flexibly.[90] The effectiveness of real-name requirements as safeguards against online abuse is questionable.[91] Indeed, strict insistence on real names has unmasked bloggers and activists using pseudonyms to protect themselves, exposing them to grave physical danger.[92] It has also blocked the accounts of lesbian, gay, bisexual, transgender and queer users and activists, drag performers and users with non-English or unconventional names.[93] Since online anonymity is often necessary for the physical safety of vulnerable users, human rights principles default to the protection of anonymity, subject only to limitations that would protect their identities.[94] Narrowly crafted impersonation rules that limit the ability of users to portray another person in a confusing or deceptive manner may be a more proportionate means of protecting the identity, rights and reputations of other users.[95]

31. *Disinformation*. Disinformation and propaganda challenge access to information and the overall public trust in media and government institutions. The companies face

[79] Julia Angwin and Hannes Grasseger, "Facebook's secret censorship rules protect white men from hate speech but not black children", ProPublica, 28 June 2017.

[80] See paras. 52 and 62 below.

[81] Twitter, "Our approach to policy development and enforcement philosophy"; YouTube policies (the importance of context); Richard Allan, "Hard questions: who should decide what is hate speech in an online global community?", Facebook Newsroom, 27 June 2017.

[82] Submissions by OBSERVACOM, p. 11 and ARTICLE 19, p. 6.

[83] WITNESS submission, pp. 6–7.

[84] Ibid.

[85] Electronic Frontier Foundation submission, p. 5.

[86] Association for Progressive Communications submission, p. 14.

[87] See Allan, "Hard questions".

[88] YouTube policies (the importance of context); Facebook community standards (hate speech).

[89] Facebook community standards (using your authentic identity). Note that Facebook now permits exceptions to its real-name policy on a case-by-case basis, but this has been criticized as insufficient: Access Now submission, p. 12. Baidu even requires the use of personally identifying information: Baidu user agreement.

[90] Twitter Help Center, "Help with username registration"; Instagram, "Getting started on Instagram".

[91] J. Nathan Matias, "The real name fallacy", Coral Project, 3 January 2017.

[92] Access Now submission, p. 11.

[93] Dia Kayyali, "Facebook's name policy strikes again, this time at Native Americans", Electronic Frontier Foundation, 13 February 2015.

[94] See A/HRC/29/32, para. 9.

[95] Twitter rules and policies (impersonation policy).

increasing pressure to address disinformation spread through links to bogus third-party news articles or websites, fake accounts, deceptive advertisements and the manipulation of search rankings.[96] However, because blunt forms of action, such as website blocking or specific removals, risk serious interference with freedom of expression, companies should carefully craft any policies dealing with disinformation.[97] Companies have adopted a variety of responses, including arrangements with third-party fact checkers, heightened enforcement of advertisement policies, enhanced monitoring of suspicious accounts, changes in content curation and search ranking algorithms, and user trainings on identifying false information.[98] Some measures, particularly those that enhance restrictions on news content, may threaten independent and alternative news sources or satirical content.[99] Government authorities have taken positions that may reflect outsized expectations about technology's power to solve such problems alone.[100]

Company moderation processes and tools

32. *Automated flagging, removal and pre-publication filtering*. The massive scale of user-generated content has led the largest companies to develop automated moderation tools. Automation has been employed primarily to flag content for human review, and sometimes to remove it. Automated tools scanning music and video for copyright infringement at the point of upload have raised concerns of overblocking, and calls to expand upload filtering to terrorist-related and other areas of content threaten to establish comprehensive and disproportionate regimes of pre-publication censorship.[101]

33. Automation may provide value for companies assessing huge volumes of user-generated content, with tools ranging from keyword filters and spam detection to hash-matching algorithms and natural language processing.[102] Hash matching is widely used to identify child sexual abuse images, but its application to "extremist" content — which typically requires assessment of context — is difficult to accomplish without clear rules regarding "extremism" or human evaluation.[103] The same is true with natural language processing.[104]

34. *User and trusted flagging*. User flags give individuals the ability to log complaints of inappropriate content with content moderators. Flags typically do not enable nuanced discussions about appropriate boundaries (e.g., why content may be offensive but, on balance, better left up).[105] They have also been "gamed" to heighten pressure on platforms to remove content supportive of sexual minorities and Muslims.[106] Many companies have developed specialized rosters of "trusted" flaggers, typically experts, high-impact users and, reportedly, sometimes government flaggers.[107] There is little or no public information

[96] Ibid.; Allen Babajanian and Christine Wendel, "#FakeNews: innocuous or intolerable?", Wilton Park report 1542, April 2017.

[97] Joint Declaration 2017.

[98] Submissions by Association for Progressive Communications, pp. 4–6 and ARTICLE 19, p. 4.

[99] Association for Progressive Communications submission, p. 5.

[100] See communication No. OL ITA 1/2018. Cf. European Commission, *A Multi-Dimensional Approach to Disinformation: Final Report of the Independent High-level Group on Fake News and Disinformation* (Luxembourg, 2018).

[101] The United Kingdom of Great Britain and Northern Ireland reportedly developed a tool to automatically detect and remove terrorist content at the point of upload. Home Office, "New technology revealed to help fight terrorist content online", 13 February 2018.

[102] Center for Democracy and Technology, *Mixed Messages? The Limits of Automated Media Content Analysis* (November 2017), p. 9.

[103] Open Technology Institute submission, p. 2.

[104] Center for Democracy and Technology, *Mixed Messages?*, p. 4.

[105] On user flags, see generally Kate Crawford and Tarleton Gillespie, "What is a flag for? Social media reporting tools and the vocabulary of complaint", *New Media and Society*, vol. 18, No. 3 (March 2016), pp. 410−428.

[106] Ibid., p. 421.

[107] YouTube Help, YouTube Trusted Flagger Program; YouTube Help, "Get involved with YouTube contributors".

explaining the selection of specialized flaggers, their interpretations of legal or community standards or their influence over company decisions.

35. *Human evaluation*. Automation often will be supplemented by human review, with the biggest social media companies developing large teams of content moderators to review flagged content.[108] Flagged content may be routed to content moderators, which will typically be authorized to make a decision — often within minutes — about the appropriateness of the content and to remove or permit it. In situations where the appropriateness of particular content is difficult to determine, moderators may escalate its review to content teams at company headquarters. In turn, company officials — typically public policy or "trust and safety" teams with the engagement of general counsel — will make decisions on removals. Company disclosure about removal discussions, in aggregate or specific cases, is limited.[109]

36. *Account or content action*. The existence of inappropriate content may trigger a range of company actions. Companies may limit content removal by jurisdiction, a range of jurisdictions, or across an entire platform or set of platforms. They may apply age limitations, warnings or demonetization.[110] Violations may lead to temporary account suspensions, while repeat offences may lead to account deactivation. In very few cases outside of copyright enforcement do the companies provide "counter-notice" procedures that permit users posting content to challenge removals.

37. *Notification*. A common complaint is that users who post reported content, or persons complaining of abuse, may not receive any notification of removal or other action.[111] Even when companies issue notifications, these typically indicate merely the action taken and a generic ground for action. At least one company has attempted to provide more context in its notifications, but it is unclear whether additional detail in stock notifications constitutes sufficient explanation in all cases.[112] Transparency and notifications go hand in hand: robust operational-level transparency that improves user awareness of the platform's approaches to content removals alleviates the pressure on notifications in individual cases, while weaker overall transparency increases the likelihood that users will be unable to understand individual removals in the absence of notifications tailored to specific cases.

38. *Appeals and remedies*. Platforms permit appeals of a range of actions, from profile or page removals to removals of specific posts, photos or videos.[113] Even with appeal, however, the remedies available to users appear limited or untimely to the point of non-existence and, in any event, opaque to most users and even civil society experts. It may be, for instance, that reinstatement of content would be an insufficient response if removal resulted in specific harm — such as reputational, physical, moral or financial — to the person posting. Similarly, account suspensions or content removals during public protest or debate could have significant impact on political rights and yet lack any company remedy.

Transparency

39. Companies have developed transparency reports that publish aggregated data on government requests for content removal and user data. Such reporting demonstrates the kinds of pressures the companies face. Transparency reporting identifies, country by

[108] See Sarah Roberts, "Commercial content moderation: digital laborers' dirty work", *Media Studies Publications*, paper 12 (2016).

[109] Cf. Wikipedia: BOLD, revert, discuss cycle. Reddit moderators are encouraged to offer "helpful rule explanations, tips and links to new and confused users" (Reddit Moddiquette).

[110] YouTube policies (nudity and sexual content policies); YouTube Help, "Creator influence on YouTube".

[111] Submissions by ARTICLE 19, p. 7 and Association for Progressive Communications, p. 16.

[112] See https://twitter.com/TwitterSafety/status/971882517698510848/.

[113] Electronic Frontier Foundation and Visualizing Impact, "How to appeal", onlinecensorship.org. Facebook and Instagram allow only the appeal of account suspensions. Cf. Github submission, p. 6.

country, the number of legal removal requests,[114] the number of requests where some action was taken or content restricted[115] and, increasingly, descriptions and examples of selected legal bases.[116]

40. However, as the leading review of Internet transparency concludes, companies disclose "the least amount of information about how *private* rules and mechanisms for self- and co-regulation are formulated and carried out".[117] In particular, disclosure concerning actions taken pursuant to private removal requests under terms of service is "incredibly low".[118] Content standards are drafted in broad terms, leaving room for platform discretion that companies do not sufficiently illuminate. Media and public scrutiny have led companies to supplement general policies with explanatory blog posts[119] and limited hypothetical examples,[120] but these fall short of illuminating nuances in how internal rules are developed and applied.[121] While terms of service are generally available in local languages, transparency reports, company blogs and related content are not, providing even less clarity to non-English-speaking users. Accordingly, users, public authorities and civil society often express dissatisfaction with the unpredictability of terms of service actions.[122] The lack of sufficient engagement, coupled with growing public criticism, has forced companies into a constant state of rule evaluation, revision and defence.

IV. Human rights principles for company content moderation

41. The founder of Facebook recently expressed his hope for a process in which the company "could more accurately reflect the values of the community in different places".[123] That process, and the relevant standards, can be found in human rights law. Private norms, which vary according to each company's business model and vague assertions of community interests, have created unstable, unpredictable and unsafe environments for users and intensified government scrutiny. National laws are inappropriate for companies that seek common norms for their geographically and culturally diverse user base. But human rights standards, if implemented transparently and consistently with meaningful user and civil society input, provide a framework for holding both States and companies accountable to users across national borders.

42. A human rights framework enables forceful normative responses against undue State restrictions — provided companies play by similar rules. The Guiding Principles and their accompanying body of "soft law" provide guidance on how companies should prevent or mitigate government demands for excessive content removals. But they also establish principles of due diligence, transparency, accountability and remediation that limit platform interference with human rights through product and policy development. Companies committed to implementing human rights standards throughout their operations — and not merely when it aligns with their interests — will stand on firmer ground when they seek to

[114] Twitter Transparency Report: Removal Requests (January−June 2017); Google Transparency Report: Government Requests to Remove Content; 2016 Reddit Inc., Transparency Report. Facebook does not provide the total number of requests received per country.

[115] See, for example, Facebook Transparency Report (France) (January−June 2017); Google Transparency Report: Government Requests to Remove Content (India); Twitter Transparency Report (Turkey).

[116] Ibid.

[117] Ranking Digital Rights submission, p. 4. Original italics.

[118] Ibid., p. 10.

[119] See Elliot Schrage, "Introducing hard questions", Facebook Newsroom, 15 June 2017; Twitter Safety, "Enforcing new rules to reduce hateful conduct and abusive behavior", 18 December 2017.

[120] See, for example, YouTube policies (violent or graphic content policies).

[121] Angwin and Grasseger, "Facebook's secret censorship rules".

[122] Submissions by Ranking Digital Rights, p. 10; OBSERVACOM p. 10; Association for Progressive Communications, p. 17; International Federation of Library Associations and Institutions, pp. 4–5, Access Now, p. 17; and EDRi, p. 5.

[123] Kara Swisher and Kurt Wagner, "Here's the transcript of Recode's interview with Facebook CEO Mark Zuckerberg about the Cambridge Analytica controversy and more", Recode, 22 March 2018.

hold States accountable to the same standards. Furthermore, when companies align their terms of service more closely with human rights law, States will find it harder to exploit them to censor content.

43. Human rights principles also enable companies to create an inclusive environment that accommodates the varied needs and interests of their users while establishing predictable and consistent baseline standards of behaviour. Amidst growing debate about whether companies exercise a combination of intermediary and editorial functions, human rights law expresses a promise to users that they can rely on fundamental norms to protect their expression over and above what national law might curtail.[124] Yet human rights law is not so inflexible or dogmatic that it requires companies to permit expression that would undermine the rights of others or the ability of States to protect legitimate national security or public order interests. Across a range of ills that may have more pronounced impact in digital space than they might offline — such as misogynist or homophobic harassment designed to silence women and sexual minorities, or incitement to violence of all sorts — human rights law would not deprive companies of tools. To the contrary, it would offer a globally recognized framework for designing those tools and a common vocabulary for explaining their nature, purpose and application to users and States.

A. Substantive standards for content moderation

44. The digital age enables rapid dissemination and enormous reach, but it also lacks textures of human context. Per the Guiding Principles, companies may take into account the size, structure and distinctive functions of the platforms they provide in assessing the necessity and proportionality of content restrictions.

45. *Human rights by default*. Terms of service should move away from a discretionary approach rooted in generic and self-serving "community" needs. Companies should instead adopt high-level policy commitments to maintain platforms for users to develop opinions, express themselves freely and access information of all kinds in a manner consistent with human rights law.[125] These commitments should govern their approach to content moderation and to complex problems such as computational propaganda[126] and the collection and handling of user data. Companies should incorporate directly into their terms of service and "community standards" relevant principles of human rights law that ensure content-related actions will be guided by the same standards of legality, necessity and legitimacy that bind State regulation of expression.[127]

46. "*Legality*". Company rules routinely lack the clarity and specificity that would enable users to predict with reasonable certainty what content places them on the wrong side of the line. This is particularly evident in the context of "extremism" and hate speech, areas of restriction easily susceptible to excessive removals in the absence of rigorous human evaluation of context. Further complicating public understanding of context-specific rules is the emerging general exception for "newsworthiness".[128] While the recognition of public interest is welcome, companies should also explain what factors are assessed in determining the public interest and what factors other than public interest inform calculations of newsworthiness. Companies should supplement their efforts to explain their rules in more detail with aggregate data illustrating trends in rule enforcement, and examples of actual cases or extensive, detailed hypotheticals that illustrate the nuances of interpretation and application of specific rules.

47. *Necessity and proportionality*. Companies should not only describe contentious and context-specific rules in more detail. They should also disclose data and examples that

[124] Global Partners Digital submission, p. 3; Guiding Principles, principle 11.
[125] Guiding Principles, principle 16.
[126] See Samuel Wooley and Philip Howard, *Computational Propaganda Worldwide: Executive Summary* (Computational Propaganda Research Project working paper No. 2017.11 (Oxford, 2017).
[127] Global Partners Digital submission, pp. 10–13.
[128] See Joel Kaplan, "Input from community and partners on our community standards", Facebook Newsroom, 21 October 2016; Twitter rules and policies.

provide insight into the factors they assess in determining a violation, its severity and the action taken in response. In the context of hate speech, explaining how specific cases are resolved may help users better understand how companies approach difficult distinctions between offensive content and incitement to hatred, or how considerations such as the intent of the speaker or the likelihood of violence are assessed in online contexts. Granular data on actions taken will also establish a basis to evaluate the extent to which companies are narrowly tailoring restrictions. The circumstances under which they apply less intrusive restrictions (such as warnings, age restrictions or demonetization) should be explained.

48. *Non-discrimination*. Meaningful guarantees of non-discrimination require companies to transcend formalistic approaches that treat all protected characteristics as equally vulnerable to abuse, harassment and other forms of censorship.[129] Indeed, such approaches would appear inconsistent with their own emphasis that context matters. Instead, when companies develop or modify policies or products, they should actively seek and take into account the concerns of communities historically at risk of censorship and discrimination.

B. Processes for company moderation and related activities

Responses to government requests

49. As company transparency reports show, Governments pressure them to remove content, suspend accounts and identify and disclose account information. Where required by local law, it may appear that companies have little choice but to comply. But companies may develop tools that prevent or mitigate the human rights risks caused by national laws or demands inconsistent with international standards.

50. *Prevention and mitigation*. Companies often claim to take human rights seriously. But it is not enough for companies to undertake such commitments internally and provide ad hoc assurances to the public when controversies arise. Companies should also, at the highest levels of leadership, adopt and then publicly disclose specific policies that "direct all business units, including local subsidiaries, to resolve any legal ambiguity in favour of respect for freedom of expression, privacy, and other human rights". Policies and procedures that interpret and implement government demands to narrow and "ensure the least restriction on content" should flow from these commitments.[130] Companies should ensure that requests are in writing, cite specific and valid legal bases for restrictions and are issued by a valid government authority in an appropriate format.[131]

51. When faced with problematic requests, companies should seek clarification or modification; solicit the assistance of civil society, peer companies, relevant government authorities, international and regional bodies and other stakeholders; and explore all legal options for challenge.[132] When companies receive requests from States under their terms of service or through other extralegal means, they should route these requests through legal compliance processes and assess the validity of such requests under relevant local laws and human rights standards.

52. *Transparency*. In the face of censorship and associated human rights risks, users can only make informed decisions about whether and how to engage on social media if interactions between companies and States are meaningfully transparent. Best practices on how to provide such transparency should be developed. Company reporting about State requests should be supplemented with granular data concerning the types of requests received (e.g., defamation, hate speech, terrorism-related content) and actions taken (e.g., partial or full removal, country-specific or global removal, account suspension, removal granted under terms of service). Companies should also provide specific examples as often

[129] See, for example, International Convention on the Elimination of All Forms of Racial Discrimination, arts. 1 (4) and 2 (2).
[130] See A/HRC/35/22, paras. 66–67.
[131] Submissions by Global Network Initiative, pp. 3–4 and GitHub, pp. 3–5.
[132] See A/HRC/35/22, para. 68.

as possible.[133] Transparency reporting should extend to government demands under company terms of service[134] and must also account for public-private initiatives to restrict content, such as the European Union Code of Conduct on countering illegal hate speech online, governmental initiatives such as Internet referral units and bilateral understandings such as those reported between YouTube and Pakistan and Facebook and Israel. Companies should preserve records of requests made under these initiatives and communications between the company and the requester and explore arrangements to submit copies of such requests to a third-party repository.

Rule-making and product development

53. *Due diligence*. Although several companies commit to human rights due diligence in assessing their response to State restrictions, it is unclear whether they implement similar safeguards to prevent or mitigate risks to freedom of expression posed by the development and enforcement of their own policies.[135] Companies should develop clear and specific criteria for identifying activities that trigger such assessments. In addition to revisions of content moderation policies and processes, assessments should be conducted on the curation of user feeds and other forms of content delivery, the introduction of new features or services and modifications to existing ones, the development of automation technologies and market-entry decisions such as arrangements to provide country-specific versions of the platform.[136] Past reporting also specifies the issues these assessments should examine and the internal processes and training required to integrate assessments and their findings into relevant operations. Additionally, these assessments should be ongoing and adaptive to changes in circumstances or operating context.[137] Multi-stakeholder initiatives such as Global Network Initiative provide an avenue for companies to develop and refine assessments and other due diligence processes.

54. *Public input and engagement*. Participants in consultations consistently raised concerns that companies failed to engage adequately with users and civil society, particularly in the global South. Input from affected rights holders (or their representatives) and relevant local or subject matter experts, and internal decision-making processes that meaningfully incorporate the feedback received, are integral components of due diligence.[138] Consultations — especially in broad forms such as calls for public comment — enable the companies to consider the human rights impact of their activities from diverse perspectives, while also encouraging them to pay close attention to how seemingly benign or ostensibly "community-friendly" rules may have significant, "hyper-local" impacts on communities.[139] For example, engagement with a geographically diverse range of indigenous groups may help companies develop better indicators for taking into account cultural and artistic context when assessing content featuring nudity.

55. *Rule-making transparency*. Companies too often appear to introduce products and rule modifications without conducting human rights due diligence or evaluating the impact in real cases. They should at least seek comment on their impact assessments from interested users and experts, in settings that guarantee the confidentiality of such assessments if necessary. They should also clearly communicate to the public the rules and processes that produced them.

---

133 See, for example, Twitter Transparency Report: Removal Requests (January−June 2017).

134 Twitter has begun to publish data on "non-legal requests submitted by known government representatives about content that may violate the Twitter Rules" prohibiting abusive behaviour, promotion of terrorism and intellectual property infringement. Ibid. See also Microsoft, Content Removal Requests Report (January−June 2017).

135 Ranking Digital Rights submission, p. 12; Guiding Principles, principle 17.

136 See A/HRC/35/22, para. 53.

137 Ibid., paras. 54−58.

138 See Guiding Principles, principle 18 and A/HRC/35/22, para. 57.

139 Chinmayi Arun, "Rebalancing regulation of speech: hyper-local content on global web-based platforms", Berkman Klein Center for Internet and Society Medium Collection, Harvard University, 2018; *Pretoria News*, "Protest at Google, Facebook 'bullying' of bare-breasted maidens", 14 December 2017.

Rule enforcement

56. *Automation and human evaluation*. Automated content moderation, a function of the massive scale and scope of user-generated content, poses distinct risks of content actions that are inconsistent with human rights law. Company responsibilities to prevent and mitigate human rights impacts should take into account the significant limitations of automation, such as difficulties with addressing context, widespread variation of language cues and meaning and linguistic and cultural particularities. Automation derived from understandings developed within the home country of the company risks serious discrimination across global user bases. At a minimum, technology developed to deal with considerations of scale should be rigorously audited and developed with broad user and civil society input.

57. The responsibility to foster accurate and context-sensitive content moderation practices that respect freedom of expression also requires companies to strengthen and ensure professionalization of their human evaluation of flagged content. This strengthening should involve protections for human moderators consistent with human rights norms applicable to labour rights and a serious commitment to involve cultural, linguistic and other forms of expertise in every market where they operate. Company leadership and policy teams should also diversify to enable the application of local or subject-matter expertise to content issues.

58. *Notice and appeal*. Users and civil society experts commonly express concern about the limited information available to those subject to content removal or account suspension or deactivation, or those reporting abuse such as misogynistic harassment and doxing. The lack of information creates an environment of secretive norms, inconsistent with the standards of clarity, specificity and predictability. This interferes with the individual's ability to challenge content actions or follow up on content-related complaints; in practice, however, the lack of robust appeal mechanisms for content removals favours users who flag over those who post. Some may argue that it will be time-consuming and costly to allow appeals on every content action. But companies could work with one another and civil society to explore scalable solutions such as company-specific or industry-wide ombudsman programmes. Among the best ideas for such programmes is an independent "social media council", modelled on the press councils that enable industry-wide complaint mechanisms and the promotion of remedies for violations.[140] This mechanism could hear complaints from individual users that meet certain criteria and gather public feedback on recurrent content moderation problems such as overcensorship related to a particular subject area. States should be supportive of scalable appeal mechanisms that operate consistently with human rights standards.

59. *Remedy*. The Guiding Principles highlight the responsibility to remedy "adverse impacts" (principle 22). However, few if any of the companies provide for remediation. Companies should institute robust remediation programmes, which may range from reinstatement and acknowledgment to settlements related to reputational or other harms. There has been some convergence among several companies in their content rules, giving rise to the possibility of inter-company cooperation to provide remedies through a social media council, other ombudsman programmes or third-party adjudication. If the failure to remediate persists, legislative and judicial intervention may be required.

60. *User autonomy*. Companies have developed tools enabling users to shape their own online environments. This includes muting and blocking of other users or specific kinds of content. Similarly, platforms often permit users to create closed or private groups, moderated by users themselves. While content rules in closed groups should be consistent with baseline human rights standards, platforms should encourage such affinity-based groups given their value in protecting opinion, expanding space for vulnerable communities and allowing the testing of controversial or unpopular ideas. Real-name requirements

[140] See ARTICLE 19, *Self-regulation and 'Hate Speech' on Social Media Platforms* (London, 2018), pp. 20−22.

should be disfavoured, given their privacy and security implications for vulnerable individuals.[141]

61. Mounting concerns about the verifiability, relevance and usefulness of information online raise complex questions about how companies should respect the right to access information. At a minimum, companies should disclose details concerning their approaches to curation. If companies are ranking content on social media feeds based on interactions between users, they should explain the data collected about such interactions and how this informs the ranking criteria. Companies should provide all users with accessible and meaningful opportunities to opt out of platform-driven curation.[142]

Decisional transparency

62. Notwithstanding advances in aggregate transparency of government removal requests, terms of service actions are largely unreported. Companies do not publish data on the volume and type of private requests they receive under these terms, let alone rates of compliance. Companies should develop transparency initiatives that explain the impact of automation, human moderation and user or trusted flagging on terms of service actions. While a few companies are beginning to provide some information about these actions, the industry should be moving to provide more detail about specific and representative cases and significant developments in the interpretation and enforcement of their policies.

63. The companies are implementing "platform law", taking actions on content issues without significant disclosure about those actions. Ideally, companies should develop a kind of case law that would enable users, civil society and States to understand how the companies interpret and implement their standards. While such a "case law" system would not involve the kind of reporting the public expects from courts and administrative bodies, a detailed repository of cases and examples would clarify the rules much as case reporting does.[143] A social media council empowered to evaluate complaints across the ICT sector could be a credible and independent mechanism to develop such transparency.

V. Recommendations

64. **Opaque forces are shaping the ability of individuals worldwide to exercise their freedom of expression. This moment calls for radical transparency, meaningful accountability and a commitment to remedy in order to protect the ability of individuals to use online platforms as forums for free expression, access to information and engagement in public life. The present report has identified a range of steps, include the following.**

Recommendations for States

65. **States should repeal any law that criminalizes or unduly restricts expression, online or offline.**

66. **Smart regulation, not heavy-handed viewpoint-based regulation, should be the norm, focused on ensuring company transparency and remediation to enable the public to make choices about how and whether to engage in online forums. States should only seek to restrict content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy. States should refrain from imposing disproportionate sanctions, whether heavy fines or imprisonment, on Internet intermediaries, given their significant chilling effect on freedom of expression.**

[141] See para. 30 above.

[142] Facebook, for example, permits users to view stories in their News Feed in reverse chronological order, but warns that it will "eventually" return to its default curation settings. Facebook Help Centre, "What's the difference between top stories and most recent stories on News Feed?".

[143] See, for example, Madeleine Varner and others, "What does Facebook consider hate speech?", ProPublica, 28 December 2017.

67. **States and intergovernmental organizations should refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship.**

68. **States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression. They should avoid delegating responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users.**

69. **States should publish detailed transparency reports on all content-related requests issued to intermediaries and involve genuine public input in all regulatory considerations.**

Recommendations for ICT companies

70. **Companies should recognize that the authoritative global standard for ensuring freedom of expression on their platforms is human rights law, not the varying laws of States or their own private interests, and they should re-evaluate their content standards accordingly. Human rights law gives companies the tools to articulate and develop policies and processes that respect democratic norms and counter authoritarian demands. This approach begins with rules rooted in rights, continues with rigorous human rights impact assessments for product and policy development, and moves through operations with ongoing assessment, reassessment and meaningful public and civil society consultation. The Guiding Principles on Business and Human Rights, along with industry-specific guidelines developed by civil society, intergovernmental bodies, the Global Network Initiative and others, provide baseline approaches that all Internet companies should adopt.**

71. **The companies must embark on radically different approaches to transparency at all stages of their operations, from rule-making to implementation and development of "case law" framing the interpretation of private rules. Transparency requires greater engagement with digital rights organizations and other relevant sectors of civil society and avoiding secretive arrangements with States on content standards and implementation.**

72. **Given their impact on the public sphere, companies must open themselves up to public accountability. Effective and rights-respecting press councils worldwide provide a model for imposing minimum levels of consistency, transparency and accountability to commercial content moderation. Third-party non-governmental approaches, if rooted in human rights standards, could provide mechanisms for appeal and remedy without imposing prohibitively high costs that deter smaller entities or new market entrants. All segments of the ICT sector that moderate content or act as gatekeepers should make the development of industry-wide accountability mechanisms (such as a social media council) a top priority.**

Chapter 38

About Freedombox

FreedomBox Foundation

About FreedomBox

The Internet Needs Freedom

The Internet is centralized and controlled by a small number of digital titans. That means that it's easy for the internet to be surveilled, data-mined, and controlled. Think about your own experience of the internet: *can you do anything on the internet without going through a major platform first?*

It's very difficult to escape the large platforms that control our data and our lives. But it shouldn't be. That's why FreedomBox was built: it cuts out the middleman and empowers you to do things like share files, send encrypted messages, have voice calls, and edit documents through a server you host yourself.

FreedomBox Creates Freedom

FreedomBox is a private server system that empowers regular people to host their own internet services, like a VPN, a personal website, file sharing, encrypted messengers, a VoIP server, a metasearch engine, and much more. It is designed to be secure, flexible, and simple. FreedomBox builds freedom into the internet by putting you in control of your activity and data on the net.

FreedomBox is made with two ingredients: (1) a free software system and (2) always-on, inexpensive, and power-efficient hardware about the size of a pocket dictionary. Though we aim for our software to be hardware-neutral, we specifically support about ten hardware models. All of our supported hardware models are single-board computers that cost about 60 USD and provide the computing power of a smart phone. The software system is 100% free and open source and available for **download at no cost.** FreedomBox is preloaded with 20+ apps and features designed to protect your freedom, privacy, and user rights.

Just install our system onto your single-board computer and plug it into your internet router. A web interface acts as the central hub, offering one-click installs and simple configuration pages for apps and services.

FreedomBox was born in 2010. After years of development, it is now a fixture in universities, villages, and homes throughout the world. FreedomBox continues to spread **thanks to our donors.**

Learn about the FreedomBox Foundation...

Chapter 39

Freedombox FAQ

Translation(s): English - Español - Français

Questions and Answers - FreedomBox

Contents

1. GENERAL INTRODUCTION

1.1. What is FreedomBox?

FreedomBox is a personal server that protects your privacy. It uses a free software stack, a subset of the Debian universal operating system, that can be installed on a variety of cheap and power-efficient hardware. FreedomBox is designed for simple set-up and operation, similar to that of a smart phone.

Continue reading on the Introduction page.

1.2. What does FreedomBox do?

FreedomBox is intended to protect your private life against advertising companies and protect your anonymity while browsing the Internet or local network. It allows you to provide services to family and friends (such as hosting files and bookmarks, remote storage, chat, wiki/blog). FreedomBox sets and upgrades automatically the security of these services. You can connect to

FreedomBox when you are outside your home in a secure manner to access services and reach other personal computers or electronic devices. You can choose to route your mobile phone traffic via your FreedomBox using your internet connection at home. You can also do group audio chats and BitTorrent, even on very simple hardware.

1.3. Can FreedomBox provide a secure email server?

Future applications include secure email server, distributed social networking, password-less single sign on, browser assistant. Active contributors are working on it. They are also working on supporting more hardware.

1.4. Do I need technical expertise to start using FreedomBox?

No, technical expertise is not required to operate FreedomBox at a high level. A turnkey FreedomBox system is available for purchase by Olimex.

1.5. What is the relationship between Debian and FreedomBox?

FreedomBox is a "pure blend" (i.e. a packaged subset) of Debian - available for some boards as a pre-installed image and generally available as a Debian package to be installed on top of an existing Debian system.

1.6. How can I ask a question?

Feel free to add your question on this page (and answer if you have it) by signing up and using the edit feature. Answers mostly come from the FreedomBox discussion list archives. Please read also live help page.

1.7. How do I communicate with users outside of my local FreedomBox?

The messaging applications and social networks on FreedomBox are federated systems; if you have an account on one server, you can talk to anyone on any server. The most common federated system is email. Just as you can send an email to users on other email servers, you can do instant messaging and social media interactions with users on other servers. For example, *ejabberd* and *Matrix Synapse* are federated instant messaging systems, while *diaspora**, *Pleroma*, *Mastodon* etc. are federated social networking systems.

2. HARDWARE (SBC)

2.1. Which single board computer (SBC) do you recommend?

Plese, read the Hardware section of the manual.

En short:

1. As **easiest** way, it is recommended to buy your pre-installed !FreedomBox from the !FreedomBox Foundation.
2. If you want to install it yourself the recommended SBC is OLinuXino A20.

   Other alternative (non pre-installed) SBC's:

   - Cubietruck / Cubieboard
   - Beaglebone Black
   - APU / ALIX

2.2. What is a single board computer (SBC)?

A single board computer (SBC) is a "mini pc" based on a single circuit board that allows a reduction of overall cost. Most of them are cheap with low energy consumption. FreedomBox is developed towards Open Source SBCs providing plug-in cards.

You can check Single-board computers page on from the the Free Software Foundation (FSF)'s hardware database.

2.3. A thing that is new to me is Open Hardware. What makes open hardware open? Anything in particular that I should be aware of?

Please use the more specific term "Open Source Hardware" or OSHW. OSHW is a definition intended to ensure your ability to "fork" a piece of hardware - i.e. pay a different factory to produce identical or derived hardware. Imagine a certain antenna vendor going bankrupt but you've created a business soldering their very particular antenna onto spaceships - when you have the "source code" for their hardware, you can pay a different vendor to produce identical antennas - and even modify them (e.g. if some particular chip inside has gone out of fashion and you want to replace it with another than requires different wiring).

"Open Hardware" is a vague term (ab)used to mean several different things related to openness of hardware. Some hardware vendors promote their boards as "open" and provide a PDF of their board design - which may be good enough to make an identical copy but not enough to fork (it is complex to rewire when you don't have the source for *computing* the layout of electrical wiring).

See discussion on the FreedomBox list.

2.4. Do I need a single board computer such as Cubietruck or Raspberry Pi?

Not necessarilly. FreedomBox may be used on any computer which you can install Debian; it may be installed via the freedombox package. But don't worry - the FreedomBox team provides images for some of the more common single board computers and for VirtualBox to make it easier for people to get up and running.

2.5. What level of performance should be expected with FreedomBox on SBCs?

Performance is not the only consideration with FreedomBox on single-board computers. The "high performance" computers *may* also consume much more energy and operate much hotter, require a fan, and therefore be noisier and potentially have a shorter operational lifespan. Different ARM devices may perform differently given the same amount of energy. For example, Allwinner-based boards of the same grade (e.g. Cubietruck and LIME2 both built around Allwinner A20) roughly perform the same, whereas Sitara-based boards (like the BeagleBone Black) are rumored to operate more efficiently in certain bases even if superficial specs may appear lower. Performance may be less important on a server than on a desktop system. The FreedomBox team believes that the Olimex A20-OLinuXino-LIME2 is currently the best option, based on its balance between performance, memory, openness and other factors. If price is more of a concern, consider the Olimex A20-OLinuXino-LIME; it has similar but slightly lower specifications of the LIME2 at a reduced price point.

If you're looking to compare the LIME and MICRO performance, both being Allwinner A20 board

from OLIMEX, see this technical benchmark (it seems to mostly depend on whether you're willing to pay 20 EUR for an extra 512 MB RAM.)

In my experience running on a BeagleBone Black, it is capable of running most day to day needs (mail, website, PHP...) except for big PHP applications like Apache+WordPress or ownCloud. They can run but are a bit sluggish. Apache and MySQL will definitely need to be tuned to use less CPU/memory.

Although a bit pricer than others, the APU 1D is probably the fastest single board computer tested so far. It has an AMD G series dual core APU, 3 Gigabit Ethernet controllers and uses Coreboot firmware.

See discussion on the FreedomBox list.

2.6. Can you recommend a WiFi adapter that leverages free firmware?

You can take a look at the wiki page USB WiFi for separate devices that do not require non-free firmware.

The MOD-WIFI-R5370-ANT from Olimex works really well, but needs a non-free firmware blob. The antenna is a bit fragile and on the MICRO, so you ought to connect it to an extension cable as the plug is quite large. If you are willing to pay more, take a look at: fsf.org, tehnoetic.com and thinkpenguin.com

The MOD-WIFI-AR9271-ANT from Olimex appears to employ a Free Software driver without the need for non-free firmware.

3. DOWNLOAD & INSTALL

3.1. General

3.1.1. What does "flashing an SD card" mean?

A Secure Digital (SD) card is a portable memory/flash card used for storage and transfer of data. An SD card uses flash memory (NOR and NAND types) that can be erased and reprogrammed. In our case, flashing an SD or microSD card means reading a binary file from your host computer and writing the file out to the card. The binary file that is written to the card will be read automatically by the bootloaded on the target computer in which the card is inserted.

3.1.2. Is FreedomBox a system in itself or must I first install Debian on a single-board computer?

The FreedomBox image is a full system image for most computer architectures. It may be installed post-Debian-install if desired.

3.1.3. What would be the benefit of first installing Debian, then FreedomBox packages?

A typical use case could be using hardware as a desktop/laptop and having FreedomBox run on the side. In this case, installing FreedomBox on Debian is a good fit. It is recommended that you install FreedomBox on a fresh Debian installation instead of an existing setup.

3.1.4. What should I know about installing FreedomBox on SBCs?

You should know that you should gather and read a lot of documentation about a first boot on your hardware. You can find documentation on the FreedomBox wiki or searching the net. Single Board Cards (SBC) have their own booting system, similar to the BIOS in x86-based computers. You should then study pre-requirements in addition to the use of FreedomBox image file. Some SBCs suffer from a lack of official documentation.

3.1.5. The SD card is not detected through USB or OTG on a Cubietruck SSD edition. Did I miss something?

Cubietruck SSD has a TransFlash (TF) slot meant to insert microSD cards on the device. SD cards will not be detected when inserted into USB based SD card readers. Cubietruck SSD with metal is tricky: please use your finger nail or any sharp object to insert the microSD card that will then latch in and lock. To release it, press again the same way.

3.1.6. How well is the Olimex A20-OLinuXino-LIME2 officially supported?

Official FreedomBox images are available for A20 OLinuXino LIME2 and MICRO since mid-October 2015. Please see discussion and download links.

3.1.7. Where can I find some documentation about a Cubietruck first boot?

You can find a document called "Cubieboard/FirstSteps" on linux-sunxi.org. The Linux-sunxi community is "an open source software community dedicated to providing open source operating system support for Allwinner SoC based devices." A system-on-a-chip (SoC) is a microchip that handle computer memory used (like RAM) to store information for immediate use. Allwinner is a particular brand of SoC processors.

3.1.8. The image I downloaded from the website seems to be broken. Can I build an image myself?

Yes, you can build your own FreedomBox images using the tool called freedom-maker. Please refer to the README.md file on how to build images yourself. Freedom-maker builds unstable images by default. You can pass your desired distribution by adding the command-line option `--distribution` (e.g. `--distribution=testing`).

3.1.9. Default username and password

FreedomBox doesn't come with a default user account. You have to connect to your FreedomBox over the network by typing the address "freedombox.local" into your web browser and create your user account from the web interface.

3.2. HowTo

3.2.1. Uninstall FreedomBox

To uninstall FreedomBox, you need to remove freedombox-setup, plinth packages and other programs you have setup using FreedomBox's web interface (Plinth). Even after that currently, not 100% will go back to normal.

3.2.2. Configuring a router to use dynamic DNS

1. Find out the mac address and current local IP of your device running

2. Open your router admistration web interface.
3. Set Up an exception for your device as a static local IP.
4. Create a port forwarding for 80 (http server) and 443 (https secure server) ports to your FreedomBox IP (made static).
5. Leave the router interface; your public IP should now provide a direct access to your FreedomBox (use http://myip.datasystems24.de to find out your public IP).

3.2.3. Create a DNS name with GnuDIP

Please read the manual and the recap on that question at the end of section.

3.2.4. Upgrade FreedomBox from stable to testing

FreedomBox is a Debian pure blend. The process for upgrading FreedomBox from stable to testing is the same as that for Debian

Steps:

Login to your FreedomBox via ssh as a user who has administrative privileges.

```
$ sudo apt edit-sources
```

Choose an editor among the options provided. Replace all instances of stable or stretch (or buster) with testing. Save and exit.

```
$ sudo apt update
$ sudo apt dist-upgrade
```

3.3. Troubleshooting

3.3.1. After the installation, I can only login via ssh with the account I had before running the FreedomBox setup script. How do I fix it?

You will need to edit /etc/security/access.conf either remove or comment out the line with "-:ALL EXCEPT root fbx (admin):ALL".

3.3.2. I'm having some problems getting FreedomBox working on a BeagleBone Black. The latest release would boot once, but after the initial reboot it wouldn't boot again.

If first boot setup is causing the further boots to fail then most likely the flash-kernel script in freedombox-setup is the reason. You can create a fresh SD card, mount it then disable by the flash-kernel script by creating a empty file in /var/freedombox/dont-tweak-kernel. Once the flash-kernel is disabled, the image should be usable and should give better chance to debug the issue for future kernel upgrades.

3.3.3. I'm trying to install FreedomBox on my Raspberry Pi 2B and FreedomBox's web interface (Plinth) does not install correctly.

You are running on Debian oldstable (jessie) which is too old to support FreedomBox. Also no one has tested FreedomBox on Raspbian yet. You have two options to run FreedomBox: Use the

FreedomBox image for Raspberry Pi 2 or Upgrade your existing image to Debian testing or unstable and then follow the FreedomBox installation process for Debian.

3.3.4. http://freedombox.local/ gives "server not found" and nmap (0 hosts up). What did I miss?

If you are logged into FreedomBox machine, you can find out the IP address directly by typing 'ip addr list'. Then connect to http://<ipaddress>/. Further more, I hope you have followed the instructions in https://wiki.debian.org/FreedomBox/Hardware/Debian. Pay particular attention to the troubleshooting item 2.

3.3.5. Why can I not login to my user? I followed the instructions on installing freedombox on Debian sid and I'm stuck with a tty login denied permission to my user account.

After running freedombox setup, it will lock out all users except: root, sudo users (in latest version), and users belonging to admin user. You can remove this restriction by removing the last line of /etc/security/access.conf No nee to run some update command after editing /etc/security/access.conf

3.3.6. Is there any reason Raspberry Pi 1 is not listed in https://www.freedombox.org/download /stable/ even though the FreedomBox images are available for Raspberry Pi 1 on the FreedomBox FTP server?

We could list the Raspberry Pi 1 image, but there are a few problems to be aware of:

- There isn't a Debian-packaged kernel for the Raspberry Pi 1. Users must run the rpi-firmware-update script on a regular basis.
- It's armel, so it's slow compared to e.g. Raspbian.
- Snapshots won't be usable, so Raspbian is recommended for running FreedomBox rather than the Raspberry Pi 1 FreedomBox image.

3.3.7. I messed up the installation of an application. Can I reinstall it somehow?

There are two parts to uninstalling an application.

- Removing the application.
- Convince FreedomBox that the application is not installed.

An example with ejabberd

Remove the application first.

```
$ sudo apt remove ejabberd
```

You can add a `--purge` before the ejabberd argument if you want to drop the database.
Then install the utility `sqlite3` to edit Plinth database file.

```
$ sudo apt install sqlite3
```

Remove the application's record from FreedomBox's database.

```
$ sudo echo "delete from plinth_module where name='ejabberd';" | sudo sqlite3 /var/li
```

Now, go back to the FreedomBox web interface and install the application.

3.3.8. A FreedomBox application has been removed from testing/stable. How do I manually install it?

You can temporarily switch to Debian unstable, install your application and go back to your previous Debian version.

SSH into your FreedomBox and run the following command to edit apt configuration.

```
$ sudo apt edit-sources
```

Replace `testing` or `stable` in the file with `unstable`. Comment out the lines containing `testing-updates` or `stretch-backports`.

```
$ sudo apt update
```

Now install the application from FreedomBox web interface. Going back

```
$ sudo apt edit-sources
```

Replace `unstable` with whatever Debian version you had before. Don't forget to uncomment the updates or backports lines that were commented earlier.

```
$ sudo apt update
```

Done.

4. USE & APPLICATIONS

4.1. General

4.1.1. Display the FreedomBox version through the User Interface

Click "?" (Help), then About.

4.2. Network Admin

4.2.1. Access your FreedomBox from the Internet

You can access your FreedomBox from the Internet after activating the Tor application. Use the given .onion address and a Tor browser for computer or a Tor app for mobile phones. You can also access your FreedomBox outside of the Tor network by using a standard IP address (http).

To configure the access from a regular http address, you need some additional setup. From your FreedomBox administration interface, go to "System Configuration" page, then "Configure" page to enter a "Domain Name". Your domain name has to be a static IP address. If your ISP does not provide you a static IP address, activate and configure "Dynamic DNS Client" in FreedomBox apps. Read the Q&A related to setting up your router and a DNS name.

4.2.2. Access FreedomBox's web interface (Plinth) from outside the local network

Access to FreedomBox's web interface (Plinth) is restricted to LAN IP addresses by default. (Note: This restriction does not apply when using a Pagekite or .onion address.) The list of restricted addresses can be found in /etc/apache2/sites-available/plinth.conf. If needed, you can add an IP address block to the <RequireAny> section, and then reload the apache2 service for it to take effect.

4.2.3. How to have a homepage on https://freedombox.local/ or the public IP

The default page is set on your machine in /etc/apache2/conf-available/freedombox.conf (the ?RedirectMatch). You can can configure this file to make freedombox.local direct to a specific landing page. It will redirect any connections that don't specify a /path.

4.2.4. I would like to configure my network statically for now. How do I do that in the "Networks"-Setting?

If you want LAN side to be configured statically, you can add a connection and choose: 1 IPv4 Addressing Method, see the manual. 2 If you want WAN side to be configured statically, you can do same but settings for default gateway and DNS Server are missing.

A page showing the current network-settings will be available in the future, see here.

4.2.5. Changing the default IP range and class

Give the following command to the network device which is configured as 'shared'.

#nmcli connection modify $CONNECTION_ID ipv4.addresses "192.168.1.0/16". $CONNECTION_ID is the id allocated to the device and to check the ID give this command. #nmcli con. IP range is determined by first IP that we allocate to the device and one can adjust the subnet too.

4.2.6. Display leased IP addresses

/var/lib/misc/dnsmasq.leases is the location to find all the IP addresses leased by FreedomBox.

4.2.7. Command-line interface: Port Forwarding in FreedomBox

The two steps which are required for enabling port forward in FreedomBox. [To make these changes permanent add --permanent to the end of both the commands.]

```
firewall-cmd --zone=external --add-port=2233/tcp
firewall-cmd --zone=external --add-forward-port=port=2233:proto=tcp:toport=22:toaddr=
```

For a detailed described check this link: "Configure Port Forwarding using the CLI".

4.3. SIP Server (repro)

4.3.1. Does anyone know the port that the SIP should be configured on?

5060 and 5061, both TCP and UDP.

4.4. Chat Server (XMPP)

4.4.1. Adding a new XMPP user

Entering a standard user in FreedomBox's web interface (Plinth) (not part of wiki nor admin group) makes the user ready to use his username@domain and password to start in any XMPP client.

4.4.2. Changing the password of a XMPP user

That is done through FreedomBox's web interface (Plinth) (Users -> select user -> Change Password form). Users will be able to connect to Plinth from an external IP address from FreedomBox version 1.0.

5. ABOUT FREEDOMBOX COMMUNITY

5.1. Contacting FreedomBox contributors

By writing to the mailing list or connecting to the IRC channel, you are addressing all the people contributing to FreedomBox. If you wish to talk to the active contributors, I suggest joining the monthly VOIP progress calls.

5.2. What is the difference between progress calls and hack calls?

The original idea was that the hack call would be less formal than progress calls. So we might have a topic of interest during hack calls, but it doesn't need to follow a set agenda.

5.3. How can I help FreedomBox get translated into my language?

Please visit Localization landing page for newcomers.

FreedomBox's user interface (UI) translation process is held on Weblate platform. The manual is created on english wiki pages and you can translate it from these documents creating local pages linked to these global pages.

6. BUSINESS

6.1. Can I use the FreedomBox logo?

Certification by the Foundation to distribute FreedomBox software is not ready yet. Please ask your question on discussion list or attending team calls. Technically speaking, you can read the documentation "FreedomBox-Identity-Manual.pdf".

FreedomBox/QuestionsAndAnswers (last modified 2019-10-08 18:15:19)

Chapter 40

Freedom in the Cloud (Eben Moglen)

Software Freedom Law Center

Freedom In the Cloud: Software Freedom, Privacy, and Security for Web 2.0 and Cloud Computing

A Speech given by Eben Moglen at a meeting of the Internet Society's New York branch on Feb 5, 2010

Event records

It's a pleasure to be here. I would love to think that the reason that we're all here on a Friday night is that my speeches are so good. I actually have no idea why we're all here on a Friday night but I'm very grateful for the invitation. I am the person who had no date tonight so it was particularly convenient that I was invited for now.

So, of course, I didn't have any date tonight. Everybody knows that. My calendar's on the web.

The problem is that problem. Our calendar is on the web. Our location is on the web. You have a cell phone and you have a cell phone network provider and if your cell phone network provider is Sprint then we can tell you that several million times last year, somebody who has a law enforcement ID card in his pocket somewhere went to the Sprint website and asked for the realtime location of somebody with a telephone number and was given it. Several million times. Just like that. We know that because Sprint admits that they have a website where anybody with a law enforcement ID can go and find the realtime location of anybody with a Sprint cellphone. We don't know that about ATT and Verizon because they haven't told us.

But that's the only reason we don't know, because they haven't told us. That's a service that you think of as a traditional service - telephony. But the deal that you get with the traditional service called telephony contains a thing you didn't know, like spying. That's not a service to you but it's a service and you get it for free with your service contract for telephony. You get for free the service of advertising with your gmail which means of course there's another service behind which is untouched by human hands, semantic analysis of your email. I still don't understand why anybody wants that. I still don't understand why anybody uses it but people do, including the very sophisticated and thoughtful people in this room.

And you get free email service and some storage which is worth exactly a penny and a half at the current price of storage and you get spying all the time.

And for free, too.

And your calendar is on the Web and everybody can see whether you have a date Friday night and you have a status - "looking" - and you get a service for free, of advertising "single: looking". Spying with it for free. And it all sort of just grew up that way in a blink of an eye and here we are. What's that got to do with open source? Well, in fact it doesn't have anything to do with open source but it has a whole lot to do with free software. Yet, another reason why Stallman was right. It's the freedom right?

So we need to back up a little bit and figure out where we actually are and how we actually got here and probably even more important, whether we can get out and if so, how? And it isn't a pretty story, at all. David's right. I can hardly begin by saying that we won given that spying comes free with everything now. But, we haven't lost. We've just really bamboozled ourselves and we're going to have to un-bamboozle ourselves really quickly or we're going to bamboozle other innocent people who didn't know that we were throwing away their privacy for them forever.

It begins of course with the Internet, which is why it's really nice to be here talking to the Internet society - a society dedicated to the health, expansion, and theoretical elaboration of a peer-to-peer network called "the Internet" designed as a network of peers without any intrinsic need for hierarchical or structural control and assuming that every switch in the Net is an independent, free-standing entity whose volition is equivalent to the volition of the human beings who want to control it.

That's the design of the NET, which, whether you're thinking about it as glued together with IPv4 or that wonderful improvement IPv6 which we will never use apparently, still assumes peer communications.

OF course, it never really really really worked out that way. There was nothing in the technical design to prevent it. Not at any rate in the technical design interconnection of nodes and their communication. There was a software

problem. It’s a simple software problem and it has a simple three syllable name. It’s name is Microsoft. Conceptually, there was a network which was designed as a system of peer nodes but the OS which occupied the network in an increasingly - I’ll use the word, they use it about us why can’t I use it back? - viral way over the course of a decade and a half. The software that came to occupy the network was built around a very clear idea that had nothing to do with peers. It was called “server client architecture”.

The idea that the network was a network of peers was hard to perceive after awhile, particularly if you were a, let us say, ordinary human being. That is, not a computer engineer, scientist, or researcher. Not a hacker, not a geek. If you were an ordinary human, it was hard to perceive that the underlying architecture of the Net was meant to be peerage because the OS software with which you interacted very strongly instantiated the idea of the server and client architecture.

In fact, of course, if you think about it, it was even worse than that. The thing called “Windows” was a degenerate version of a thing called “X Windows”. It, too, thought about the world in a server client architecture, but what we would now think of as now backwards. The server was the thing at the human being’s end. That was the basic X Windows conception of the world. it’s served communications with human beings at the end points of the Net to processes located at arbitrary places near the center in the middle, or at the edge of the NET. It was the great idea of Windows in an odd way to create a political archetype in the Net which reduced the human being to the client and produced a big, centralized computer, which we might have called a server, which now provided things to the human being on take-it-or-leave-it terms.

They were, of course, quite take-it or leave-it terms and unfortunately, everybody took it because they didn’t know how to leave once they got in. Now the Net was made of servers in the center and clients at the edge. Clients had rather little power and servers had quite a lot. As storage gets cheaper, as processing gets cheaper, and as complex services that scale in ways that are hard to use small computers for - or at any rate, these aggregated collections of small computers for - the most important of which is search. As services began to populate that net, the hierarchical nature of the Net came to seem like it was meant to be there. The Net was made of servers and clients and the clients were the guys at the edge representing humans and servers were the things in the middle with lots of power and lots of data.

Now, one more thing happened about that time. It didn’t happen in Microsoft Windows computers although it happened in Microsoft Windows servers and it happened more in sensible OSs like Unix and BSD and other ones. Namely, servers kept logs. That’s a good thing to do. Computers ought to keep logs. It’s a very wise decision when creating computer OS software to keep logs. It helps with debugging, makes efficiencies attainable, makes it possible to study the actual operations of computers in the real world. It’s a very good idea.

But if you have a system which centralizes servers and the servers centralize their logs, then you are creating vast repositories of hierarchically organized data about people at the edges of the network that they do not control and, unless they are experienced in the operation of servers, will not understand the comprehensiveness of, the meaningfulness of, will not understand the aggregatability of.

So we built a network out of a communications architecture design for peering which we defined in client-server style, which we then defined to be the dis-empowered client at the edge and the server in the middle. We aggregated processing and storage increasingly in the middle and we kept the logs - that is, info about the flows of info in the Net - in centralized places far from the human beings who controlled or thought they controlled the operation of the computers that increasingly dominated their lives. This was a recipe for disaster.

This was a recipe for disaster. Now, I haven't mentioned yet the word "cloud" which I was dealt on the top of the deck when I received the news that I was talking here tonight about privacy and the cloud.

I haven't mentioned the word "cloud" because the word "cloud" doesn't really mean anything very much. In other words, the disaster we are having is not the catastrophe of the cloud. The disaster we are having is the catastrophe of the way we misunderstood the Net under the assistance of the un-free software that helped us to understand it. What "cloud" means is that servers have ceased to be made of iron. "Cloud" means virtualization of servers has occurred.

So, out here in the dusty edges of the galaxy where we live in dis-empowered clienthood, nothing very much has changed. As you walk inward towards the center of the galaxy, it gets more fuzzy than it used to. We resolve now halo where we used to see actual stars. Servers with switches and buttons you can push and such. Instead, what has happened is that iron no longer represents a single server. Iron is merely a place where servers could be. So "cloud" means servers have gained freedom, freedom to move, freedom to dance, freedom to combine and separate and re-aggregate and do all kinds of tricks. Servers have gained freedom. Clients have gained nothing. Welcome to the cloud.

It's a minor modification of the recipe for disaster. It improves the operability for systems that control the clients out there who were meant to be peers in a Net made of equal things.

So that's the architecture of the catastrophe. If you think about it, each step in that architectural revolution: from a network made of peers, to servers that serve the communication with humans, to clients which are programs running on heavy iron, to clients which are the computers that people actually use in a fairly dis-empowered state and servers with a high concentration of power in the Net, to servers as virtual processes running in clouds of iron at the center of an increasingly hot galaxy and the clients are out there in the dusty spiral arms.

All of those decisions architecturally were made without any discussion of the social consequences long-term, part of our general difficulty in talking about the social consequences of technology during the great period of invention of the Internet done by computer scientists who weren't terribly interested in Sociology, Social Psychology, or, with a few shining exceptions - freedom. So we got an architecture which was very subject to misuse. Indeed, it was in a way begging to be misused and now we are getting the misuse that we set up. Because we have thinned the clients out further and further and further. In fact, we made them mobile. We put them in our pockets and we started strolling around with them.

There are a lot of reasons for making clients dis-empowered and there are even more reasons for dis-empowering the people who own the clients and who might quaintly be thought of the people who ought to control them. If you think for just a moment how many people have an interest in dis-empowering the clients that are the mobile telephones you will see what I mean. There are many overlapping rights owners as they think of themselves each of whom has a stake in dis-empowering a client at the edge of the network to prevent particular hardware from being moved from one network to another. To prevent particular hardware from playing music not bought at the great monopoly of music in the sky. To disable competing video delivery services in new chips I founded myself that won't run popular video standards, good or bad. There are a lot of business models that are based around mucking with the control over client hardware and software at the edge to deprive the human that has quaintly thought that she purchased it from actually occupying the position that capitalism says owners are always in - that is, of total control.

In fact, what we have as I said a couple of years ago in between appearances here at another NYU function. In fact, what we have are things we call platforms. The word "platform" like the word "cloud" doesn't inherently mean anything. It's thrown around a lot in business talk. But, basically what platform means is places you can't leave. Stuff you're stuck to. Things that don't let you off. That's platforms. And the Net, once it became a hierarchically architected zone with servers in the center and increasingly dis-empowered clients at the edge, becomes the zone of platforms and platform making becomes the order of the day.

Some years ago a very shrewd lawyer who works in the industry said to me "Microsoft was never really a software company. Microsoft was a platform management company". And I thought Yes, shot through the heart.

So we had a lot of platform managers in a hierarchically organized network and we began to evolve services. "Services" is a complicated word. It's not meaningless by any means but it's very tricky to describe it. We use it for a lot of different things. We badly need an analytical taxonomy of "services" as my friend and colleague Philippe Aigrain in Paris pointed out some 2 or 3 years ago. Taxonomies of "services" involve questions of simplicity, complexity, scale, and

control.

To take an example, we might define a dichotomy between complex and simple services in which simple services are things that any computer can perform for any other computer if it wants to and complex services are things you can't do with a computer. You must do with clusters or structures of some computational or administrative complexity. SEARCH is a complex service. Indeed, search is the archetypal complex service. Given the one way nature of links in the Web and other elements in the data architecture we are now living with (that's another talk, another time) search is not a thing that we can easily distribute. The power in the market of our friends at Google depends entirely on the fact that search is not easily distributed. It is a complex service that must be centrally organized and centrally delivered. It must crawl the web in a unilateral direction, link by link, figuring out where everything is in order to help you find it when you need it. In order to do that, at least so far, we have not evolved good algorithmic and delivery structures for doing it in a decentralized way. So, search becomes an archetypal complex service and it draws onto itself a business model for its monetiztion.

Advertising in the 20th century was a random activity. You threw things out and hoped they worked. Advertising in the 21st century is an exquisitely precise activity. You wait for a guy to want something and then you send him advertisements about what he wants and bingo it works like magic. So of course on the underside of a complex service called search there is a theoretically simple service called advertising which, when unified to a complex service, increases its efficiency by orders of magnitude and the increase of the efficiency of the simple service when combined with the complex one produces an enormous surplus revenue flow which can be used to strengthen search even more.

But that's the innocent part of the story and we don't remain in the innocent part of the story for a variety of uses. I won't be tedious on a Friday night and say it's because the bourgeoisie is constantly engaged in destructively reinventing and improving its own activities and I won't be moralistic on a Friday night that you can't do that and say because sin is in-eradicable and human beings are fallen creatures and greed is one of the sins we cannot avoid committing. I will just say that as a sort of ordinary social process we don't stop at innocent. We go on, which surely is the thing you should say on a Friday night. And so we went on.

Now, where we went on is really towards the discovery that all of this would be even better if you had all the logs of everything because once you have the logs of everything then every simple service is suddenly a goldmine waiting to happen and we blew it because the architecture of the Net put the logs in the wrong place. They put the logs where innocence would be tempted. They put the logs where the failed state of human beings implies eventually bad trouble and we got it.

The cloud means that we can't even point in the direction of the server anymore and because we can't even point in the direction of the server anymore we don't have extra technical or non-technical means of reliable control over this disaster in slow motion. You can make a rule about logs or data flow or preservation or control or access or disclosure but your laws are human laws and they occupy particular territory and the server is in the cloud and that means the server is always one step ahead of any rule you make or two or three or six or poof! I just realized I'm subject to regulation, I think I'll move to Oceana now.

Which means that in effect, we lost the ability to use either legal regulation or anything about the physical architecture of the network to interfere with the process of falling away from innocence that was now inevitable in the stage I'm talking about, what we might call late Google stage 1.

It is here, of course, that Mr. Zuckerberg enters.

The human race has susceptibility to harm but Mr. Zuckerberg has attained an unenviable record: he has done more harm to the human race than anybody else his age.

Because he harnessed Friday night. That is, everybody needs to get laid and he turned it into a structure for degenerating the integrity of human personality and he has to a remarkable extent succeeded with a very poor deal. Namely, "I will give you free web hosting and some PHP doodads and you get spying for free all the time". And it works.

That's the sad part, it works.

How could that have happened?

There was no architectural reason, really. There was no architectural reason really. Facebook is the Web with "I keep all the logs, how do you feel about that?" It's a terrarium for what it feels like to live in a panopticon built out of web parts.

And it shouldn't be allowed. It comes to that. It shouldn't be allowed. That's a very poor way to deliver those services. They are grossly overpriced at "spying all the time". They are not technically innovative. They depend upon an architecture subject to misuse and the business model that supports them is misuse. There isn't any other business model for them. This is bad.

I'm not suggesting it should be illegal. It should be obsolete. We're technologists, we should *fix* it.

I'm glad I'm with you so far. When I come to how we should fix it later I hope you will still be with me because then we could get it done.

But let's say, for now, that that's a really good example of where we went wrong and what happened to us because. It's trickier with gmail because of that magical untouched by human hands-iness. When I say to my students, "why do you let people read your email", they say "but nobody is reading my email, no human being ever touched it. That would freak me out, I'd be creeped out if guys at Google were reading my email. But that's not happening so I don't have a problem."

Now, this they cannot say about Facebook. Indeed, they know way too much about Facebook if they let themselves really know it. You have read the stuff and you know. Facebook workers know who's about to have a love affair before the people do because they can see X obsessively checking the Facebook page of Y. There's some very nice research done a couple of years ago at an MIT I shouldn't name by students I'm not going to describe because they were a little denting to the Facebook terms of service in the course of their research. They were just scraping but the purpose of their scraping was the demonstrate that you could find closeted homosexuals on Facebook.

They don't say anything about their sexual orientation. Their friends are out, their interests are the interests of their friends who are out. Their photos are tagged with their friends who are out and they're out except they're not out. They're just out in Facebook if anybody looks, which is not what they had in mind surely and not what we had in mind for them, surely. In fact, the degree of potential information inequality and disruption and difficulty that arises from a misunderstanding, a heuristic error, in the minds of human beings about what is and what's not discoverable about them is not our biggest privacy problem.

My students, and I suspect many of the students of teachers in this room too, show constantly in our dialog the difficulty. They still think of privacy as "the one secret I don't want revealed" and that's not the problem. Their problem is all the stuff that's the cruft, the data dandruff of life, that they don't think of as secret in any way but which aggregates to stuff that they don't want anybody to know. Which aggregates, in fact, not just to stuff they don't want people to know but to predictive models about them that they would be very creeped out could exist at all. The simplicity with which you can de-anonymize theoretically anonymized data, the ease with which, for multiple sources available to you through third and fourth party transactions, information you can assemble, data maps of people's lives. The ease with which you begin constraining, with the few things you know about people, the data available to you, you can quickly infer immense amounts more.

My friend and colleague Bradley Kuhn who works at the Software Freedom Law Center is one of those archaic human beings who believes that a social security number is a private thing. And he goes to great lengths to make sure that his Social Security is not disclosed which is his right under our law, oddly enough. Though, try and get health insurance or get a safe deposit box, or in fact, operate the business at all. We bend over backwards sometimes in the operation

of our business because Bradley's Social Security number is a secret. I said to him one day "You know, it's over now because Google knows your Social Security number". He said "No they don't, I never told it to anybody". I said, "Yeah but they know the Social Security number of everybody else born in Baltimore that year. Yours is the other one".

And as you know, that's true. The data that we infer is the data in the holes between the data we already know if we know enough things.

So, where we live has become a place in which it would be very unwise to say about anything that it isn't known. If you are pretty widely known in the Net and all of us for one reason or another are pretty widely known in the Net. We want to live there. It is our neighborhood. We just don't want to live with a video camera on every tree and a mic on every bush and the data miner beneath our feet everywhere we walk and the NET is like that now. I'm not objecting to the presence of AOL newbies in Usenet news. This is not an aesthetic judgment from 1995 about how the neighborhood is now full of people who don't share our ethnocentric techno geekery. I'm not lamenting progress of a sort of democratizing kind. On the contrary, I'm lamenting progress of a totalizing kind. I'm lamenting progress hostile to human freedom. We all know that it's hostile to human freedom. We all understand it's despotic possibilities because the distopias of which it is fertile were the stuff of the science fiction that we read when we were children. The Cold War was fertile in the fantastic invention of where we live now and it's hard for us to accept that but it's true. Fortunately, of course, it's not owned by the government. Well, it is. It's fortunate. It's true. It's fortunate that it's owned by people that you can bribe to get the thing no matter who you are. If you're the government you have easy ways of doing it. You fill out a subpoena blank and you mail it.

I spent two hours yesterday with a law school class explaining in detail why the 4th Amendment doesn't exist anymore because that's Thursday night and who would do that on a Friday night? But the 4th Amendment doesn't exist anymore. I'll put the audio on the Net and the FBI and you can listen to it anytime you want.

We have to fess up if we're the people who care about freedom, it's late in the game and we're behind. We did a lot of good stuff and we have a lot of tools lying around that we built over the last 25 years. I helped people build those tools. I helped people keep those tools safe, I helped people prevent the monopoly from putting all those tools in its bag and walking off with them and I'm glad the tools are around but we do have to admit that we have not used them to protect freedom because freedom is decaying and that's what David meant in his very kind introduction.

In fact, people who are investing in the new enterprises of unfreedom are also the people you will hear if you hang out in Silicon Valley these days that open source has become irrelevant. What's their logic? Their logic is that software as

a service is becoming the way of the world. Since nobody ever gets any software anymore, the licenses that say “if you give people software you have to give them freedom” don’t matter because you’re not giving anybody software. You’re only giving them services.

Well, that’s right. Open source doesn’t matter anymore. Free software matters a lot because of course, free software is open source software with freedom. Stallman was right. It’s the freedom that matters. The rest of it is just source code. Freedom still matters and what we need to do is to make free software matter to the problem that we have which is unfree services delivered in unfree ways really beginning to deteriorate the structure of human freedom.

Like a lot of unfreedom, the real underlying social process that forces this unfreedom along is nothing more than perceived convenience.

All sorts of freedom goes over perceived convenience. You know this. You’ve stopped paying for things with cash. You use a card that you can wave at an RFID reader.

Convenience is said to dictate that you need free web hosting and PHP doodads in return for spying all the time because web servers are so terrible to run. Who could run a web server of his own and keep the logs? It would be brutal. Well, it would if it were IIS. It was self-fulfilling, it was intended to be. It was designed to say “you’re a client, I’m a server. I invented Windows 7, It was my idea. I’ll keep the logs thank you very much.” That was the industry. We built another industry. It’s in here. But it’s not in. Well, yeah it is kind of in here. So where isn’t it? Well it’s not in the personal web server I don’t have that would prevent me from falling…well, why don’t we do something about that.

What do we need? We need a really good webserver you can put in your pocket and plug in any place. In other words, it shouldn’t be any larger than the charger for your cell phone and you should be able to plug it in to any power jack in the world and any wire near it or sync it up to any wifi router that happens to be in its neighborhood. It should have a couple of USB ports that attach it to things. It should know how to bring itself up. It should know how to start its web server, how to collect all your stuff out of the social networking places where you’ve got it. It should know how to send an encrypted backup of everything to your friends’ servers. It should know how to microblog. It should know how to make some noise that’s like tweet but not going to infringe anybody’s trademark. In other words, it should know how to be you …oh excuse me I need to use a dangerous word - avatar - in a free net that works for you and keeps the logs. You can always tell what’s happening in your server and if anybody wants to know what’s happening in your server they can get a search warrant.

And if you feel like moving your server to Oceana or Sealand or New Zealand or the North Pole, well buy a plane ticket and put it in your pocket. Take it there. Leave it behind. Now there’s a little more we need to do. It’s all trivial. We need

some dynamic DNS and all stuff we've already invented. It's all there, nobody needs anything special. Do we have the server you can put in your pocket? Indeed, we do. Off the shelf hardware now. Beautiful little wall warts made with ARM chips. Exactly what I specked for you. Plug them in, wire them up. How's the software stack in there? Gee, I don't know it's any software stack you want to put in there.

In fact, they'll send it to you with somebody's top of the charts current distro in it, you just have to name which one you want. Which one do you want? Well you ought to want the Debian Gnu Linux social networking stack delivered to you free, free as in freedom I mean. Which does all the things I name - brings itself up, runs it's little Apache or lighttpd or it's tiny httpd, does all the things we need it to do - syncs up, gets your social network data from the places, slurps it down, does your backup searches, finds your friends, registers your dynamic DNS. All is trivial. All this is stuff we've got. We need to put this together. I'm not talking about a thing that's hard for us. We need to make a free software distribution device. How many of those do we do?

We need to give a bunch to all our friends and we need to say, here fool around with this and make it better. We need to do the one thing we are really really really good at because all the rest of it is done, in the bag, cheap ready. Those wall wart servers are $99 now going to $79 when they're five million of them they'll be $29.99.

Then we go to people and we say $29.99 once for a lifetime, great social networking, updates automatically, software so strong you couldn't knock it over it you kicked it, used in hundreds of millions of servers all over the planet doing a wonderful job. You know what? You get "no spying" for free. They want to know what's going on in there? Let them get a search warrant for your home, your castle, the place where the 4th Amendment still sort of exists every other Tuesday or Thursday when the Supreme Court isn't in session. We can do that. We can do that. That requires us to do only the stuff we're really really good at. The rest of it we get for free. Mr. Zuckerberg? Not so much.

Because of course, when there is a competitor to "all spying all the time whether you like it or not", the competition is going to do real well. Don't expect Google to be the competitor. That's our platform. What we need is to make a thing that's so greasy there will never be a social network platform again. Can we do it? Yeah, absolutely. In fact, if you don't have a date on Friday night, let's just have a hackfest and get it done. It's well within our reach.

We're going to do it before the Facebook IPO? Or are we going to wait till after? Really? Honestly? Seriously. The problem that the law has very often in the world where we live and practice and work, the problem that the law has very often, the problem that technology can solve. And the problem that technology can solve is the place where we go to the law. That's the free software movement. There's software hacking over here and there's legal hacking over

there and you put them both together and the whole is bigger than the sum of the parts. So, it's not like we have to live in the catastrophe. We don't have to live in the catastrophe. It's not like what we have to do to begin to reverse the catastrophe is hard for us. We need to re-architect services in the Net. We need to re-distribute services back towards the edge. We need to de-virtualize the servers where your life is stored and we need to restore some autonomy to you as the owner of the server.

The measures for taking those steps are technical. As usual, the box builders are ahead of us. The hardware isn't the constraint. As usual, nowadays, the software isn't really that deep a constraint either because we've made so much wonderful software which is in fact being used by all the guys on the bad architecture. They don't want to do without our stuff. The bad architecture is enabled, powered by us. The re-architecture is too. And we have our usual magic benefit. If we had one copy of what I'm talking about, we'd have all the copies we need. We have no manufacturing or transport or logistics constraint. If we do the job, it's done. We scale.

This is technical challenge for social reason. It's a frontier for technical people to explore. There is enormous social pay-off for exploring it.

The payoff is plain because the harm being ameliorated is current and people you know are suffering from it. Everything we know about why we make free software says that's when we come into our own. It's a technical challenge incrementally attainable by extension from where we already are that makes the lives of the people around us and whom we care about immediately better. I have never in 25 years of doing this work, I have never seen us fail to rise to a challenge that could be defined in those terms. So I don't think we're going to fail this one either.

Mr. Zuckerberg richly deserves bankruptcy.

Let's give it to him. For Free.

And I promise, and you should promise too, not to spy on the bankruptcy proceeding. It's not any of our business. It's private.

This is actually a story potentially happy. It is a story potentially happy and if we do it then we will have quelled one more rumor about the irrelevance of us and everybody in the Valley will have to go find another buzz word and all the guys who think that Sandhill Road is going to rise into new power and glory by spying on everybody and monetizing it will have to find another line of work too, all of which is purely on the side of the angels. Purely on the side of the angels.

We will not be rid of all our problems by any means, but just moving the logs from them to you is the single biggest step that we can take in resolving a whole range of social problems that I feel badly about what remains of my American constitution and that I would feel badly about if I were watching the

failure of European data protection law from inside instead of outside and that I would feel kind of hopeful about if I were, oh say, a friend of mine in China. Because you know of course we really ought to put a VPN in that wall wart.

And probably we ought to put a Tor router in there.

And of course, we've got bittorrent, and by the time you get done with all of that, we have a freedom box. We have a box that not merely climbs us out of the hole we're in, we have a box that actually puts a ladder up for people who are deeper in the hole than we are, which is another thing we love to do.

I do believe the US State Department will go slanging away at the Chinese communist party for a year or two about internet freedom and I believe the Chinese communist party is going to go slanging back and what they're going to say is "You think you've got real good privacy and autonomy in the internet voyear in your neighborhood?" And every time they do that now as they have been doing that in the last 2 weeks, I would say ouch if I was Hilary Clinton and I knew anything about it because we don't. Because we don't. It's true. We have a capitalist kind and they have a centralist vanguard of the party sort of Marxist kind or maybe Marxist or maybe just totalitarian kind but we're not going to win the freedom of the net discussion carrying Facebook on our backs. We're not.

But you screw those wall wart servers around pretty thickly in American society and start taking back the logs and you want to know who I talked to on a Friday night? Get a search warrant and stop reading my email. By the way there's my GPG key in there and now we really are encrypting for a change and so on and so on and so on and it begins to look like something we might really want to go on a national crusade about. We really are making freedom here for other people too. For people who live in places where the web don't work.

So there's not a challenge we don't want to rise to. It's one we want to rise to plenty. In fact, we're in a happy state in which all the benefits we can get are way bigger than the technical intricacy of doing what needs to be done, which isn't much.

That's where we came from. We came from our technology was more free than we understood and we gave away a bunch of the freedom before we really knew it was gone. We came from unfree software had bad social consequences further down the road than even the freedom agitators knew. We came from unfreedom's metaphors tend to produce bad technology.

In other words, we came from the stuff that our movement was designed to confront from the beginning but we came from there. And we're still living with the consequences of we didn't do it quite right the first time, though we caught up thanks to Richard Stallman and moving on.

Where we live now is no place we're going to have to see our grandchildren live. Where we live now is no place we would like to conduct guided tours of. I

used to say to my students how many video cameras are there between where you live and the Law school? Count them. I now say to my students how many video cameras are there between the front door to the law school and this classroom? Count them.

I now say to my students “can you find a place where there are no video cameras?” Now, what happened in that process was that we created immense cognitive auxiliaries for the state - enormous engines of listening. You know how it is if you live in an American university thanks to the movie and music companies which keep reminding you of living in the midst of an enormous surveillance network. We’re surrounded by stuff listening to and watching us. We’re surrounded by mine-able data.

Not all of that’s going to go away because we took Facebook and split it up and carried away our little shards of it. It’s not going to go away cause we won’t take free webhosting with spying inside anymore. We’ll have other work to do. And some of that work is lawyers work. I will admit that. Some of that work is law drafting and litigating and making trouble and doing lawyer stuff. That’s fine. I’m ready.

My friends an I will do the lawyers part. It would be way simpler to do the lawyer’s work if we were living in a society which had come to understand it’s privacy better. It would be way simpler to do the lawyer’s work if young people realize that when they grow up and start voting or start voting now that they’re grown up, this is an issue. That they need to get the rest of it done the way we fixed the big stuff when we were kids. We’ll have a much easier time with the enormous confusions of international interlocking of regimes when we have deteriorated the immense force of American capitalism forcing us to be less free and more surveilled for other people’s profit all the time. It isn’t that this gets all the problems solved but the easy work is very rich and rewarding right now.

The problems are really bad. Getting the easy ones out will improve the politics for solving the hard ones and it’s right up our alley. The solution is made of our parts. We’ve got to do it. That’s my message. It’s Friday night. Some people don’t want to go right back to coding I’m sure. We could put it off until Tuesday but how long do you really want to wait? You know everyday that goes by there’s more data we’ll never get back. Everyday that goes by there’s more data inferences we can’t undo. Everyday that goes by we pile up more stuff in the hands of the people who got too much. So it’s not like we should say “one of these days I’ll get around to that”. It’s not like we should say “I think I’d rather sort of spend my time browsing news about iPad”.

It’s way more urgent than that.

It’s that we haven’t given ourselves the direction in which to go so let’s give ourselves the direction in which to go. The direction in which to go is freedom using free software to make social justice.

But, you know this. That’s the problem with talking on a Friday night. You talk for an hour and all you tell people is what they know already.

So thanks a lot. I’m happy to take your questions.

Search