Software Freedom
Law Center

Software Freedom Law Center

Fall Conference
at Columbia Law School

CLE materials

October 30, 2015

License Compliance Dispute Resolution

Software Freedom Law Center
October 30, 2015

1) Software Freedom Law Center: Guide to GPL Compliance 2nd Edition

2) Free Software Foundation: Principles for Community-Oriented GPL Enforcement

3) Terry J. Ilardi: FOSS Compliance @ IBM 15 Years (and counting)

Software Freedom Law Center Guide to GPL Compliance
2nd Edition

Eben Moglen & Mishi Choudhary

October 31, 2014

Contents

The What, Why and How of GNU GPL 3
- Copyright and Copyleft 4
- Concepts and License Mechanics of Copyleft 6

License Provisions Analyzed 10
- GPLv2 10
- GPLv3 18
- GPL Special Exception Licenses 31
- AGPL 31
- LGPL 34

Understanding Your Compliance Responsibilities 41
- Who Has Compliance Obligations? 41

How to Meet Compliance Obligations 43
- The Key to Compliance is Governance 45
- Principles of Prepared Compliance 47

Handling Compliance Inquiries 48

Appendix 1: Offer of Source Code 52

References 56

This document presents the legal analysis of the Software Freedom Law Center and the authors. This document does not express the views, intentions, policy, or legal analysis of any SFLC clients or client organizations. This document does not constitute legal advice or opinion regarding any specific factual situation or party. Specific legal advice should always be sought from qualified legal counsel on the application of the law in any particular circumstances.

©2014, Software Freedom Law Center. Licensed under the Creative Commons Attribution-ShareAlike 4.0 International (CC-BY-SA 4.0) License.

SFLC first published its guide to compliance with the GNU GPL and related licenses in 2008. We think that after six years of further adoption of GPL'd software, including the immense success of Android and other systems relying upon GPL'd software embedded in devices, it is time for a major revision of our advice on the subject. The changes that have occurred in the industrial use of copylefted software over the last decade make different emphasis necessary. This version of the Guide contains a clause by clause analysis of the compliance obligations created by each of the GNU GPL family of licenses,[1] to provide clear legal guidance on the licenses' requirements. Introducing that analysis, however, we begin by describing the underlying concepts of copyleft, which may be particularly helpful to newcomers to the subject. We also want to emphasize *software governance*, the general business processes for taking in, using, modifying and emitting third-party software, which have become far more relevant to businesses large and small. In the final chapter of this Guide, therefore, we discuss the relation of governance to compliance, and provide direct practical advice about responding to inquiries or compliance complaints from copyright holders.

The What, Why and How of GNU GPL

There are several major types of free or open source software licenses. Many of those licenses, which are known conventionally as "permissive," or "weak copyleft" licenses are concerned with preserving the freedoms of programmers. The "copyleft" licenses of the Free Software Foundation, which are the subject of this document, are concerned with protecting the freedoms of programmers, but more importantly they protect the freedoms of all *users*. The goal of the copyleft licenses is to ensure that all users of a program, or any work based on the program, have four fundamental freedoms:

0. The freedom to run the program for any purpose, without any additional permission;

[1] This document is about compliance with the GNU family of licenses, namely, GNU General Public License (GPL) versions 2 & 3, Lesser General Public License (LGPL) versions 2.1 & 3, Affero General Public License (AGPL)version 1 & 3. Many of our comments address all of these licenses and we refer to them as "the licenses" or "GNU licenses". When we are speaking of a particular license or a particular version, we refer to it in its short form along with the version number. In accord with longstanding free software community usage, we use "GPL'd" to mean "licensed under the GPL".

1. The freedom to read, study, understand and use any know-how or techniques taught or contained by the source code of the program;
2. The freedom to modify, adapt, improve, or reuse any or all of the program code; and
3. The freedom to share with anyone, or no one, both modified and unmodified versions of the program.

The easiest way to understand license terms is to begin with *why*, rather than *what*. The GNU licenses have been written by developers and their lawyers for application by developers without any aid or assistance from lawyers, for the purpose of assuring these freedoms to all their users, and all users of modified versions or new programs containing portions of their programs. The essence of these freedoms is the prevention of proprietary enhancements to copylefted programs. If a GPL'd program can be enhanced with proprietary code, however packaged or however written, then the intentions of the developers to protect users' rights will be frustrated. The *why* of copyleft, then, is to protect all downstream users' freedoms by prohibiting proprietary enhancement. As the Preamble of GPLv3 puts it,

> To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

This document explains what those responsibilities are, and how to discharge them most productively for users, at least cost to intermediate users, modifiers, packagers and resellers.

Copyright and Copyleft

The primary legal regime that applies to software is copyright law. Copyleft, which uses functional parts of copyright law to achieve an unusual result (legal protection for free sharing) forms the core legal principle of these licenses. It modifies, or "hacks" copyright law, which is usually employed to strengthen the rights of authors or publishers, to strengthen instead the rights of users.

Any work that is based on a copylefted program must also be licensed under the same copyleft license. This is sometimes referred to as the "hereditary

effect" of copyleft or "share and share alike" principle. This "reciprocity" or "share and share alike" rule protects both developers, who avoid facing a "proprietized" competitor of their project, and users, who can be sure that they will have all four basic freedoms not only in the present version of the program they use, but in all its future improved versions.

In order to implement users' freedoms to study, modify and share, all users of GPL'd programs who receive binary or executable copies are entitled to receive complete and corresponding source code (C&CS). If C&CS is not provided along with the binaries, a written offer to provide C&CS must accompany the binary copy, irrespective of the medium of software distribution. This requirement to provide or offer C&CS is basic to the protection of users' rights.[2] Satisfying this requirement is also the most important component of license compliance. The licenses' requirement for the provision of C&CS is exacting: the supplier of binaries must supply or offer all the source code, makefiles, and other building materials required to produce the binary executable received by the user.

Unless every individual user is free to fix bugs, enhance features, and reuse code, users are deprived of the full value of the software that authors intended for them to have. If the license terms are not enforced, then proprietary enhancements will eventually come to represent the state of the art, as the copyleft program is submerged under the subsequent layers of proprietary enhancement. The source code requirement therefore applies whether users receive software in the form of digital transmissions over a network, as bits fixated in computer-readable media, or as software embedded in physical devices. The form of software has no effect on the extent or quality of the rights of the users.

Copyright law grants exclusive rights to authors. The "preclusive" use of copyleft to protect users' rights still leaves the authors, as copyright holders, or their agents in the sole position of enforcers or protectors of their users' rights. Actions for copyright infringement are the ultimate legal mechanism for enforcement, and copyright law allows only a copyright holder or her agent to bring an action for infringement. There also exist community efforts at compliance that help copyright holders in enforcement of their rights, but

[2] Parties who criticize copyleft or the GPL for making this requirement "viral" may well believe that programmers should be allowed to do whatever they want with code. They may thus see licenses without the source code requirement as "more free." But if the goal of the license is to protect *users* rights, then the requirement to provide complete source code is unavoidable: without the source code, no freedoms of *users* can be effectively protected.

only the copyright holders or their legal representatives can actually initiate enforcement proceedings in the legal system.

Concepts and License Mechanics of Copyleft

In our experience working with communities and companies, we have encountered numerous misconceptions about the GNU licenses' terms and core concepts. In this section we show how the working parts of the licenses implement the basic concepts upon which copyleft is based, followed by an explanation of specific terms of each license and how those terms impose specific compliance obligations. What may at first seem arbitrary or counter-intuitive becomes easier to grasp if your constant reference point is the intention of the licenses and the core concepts that they are based upon.

"The Work" and Copyleft

The unit of copyright law is "the work." In that sense, the "work" referenced by the licenses is anything that can be copyrighted or will be subject to the terms of copyright law. The GNU licenses exercise their scope fully. Anything which is "a work" or a "work based on a work" licensed under GPL is subject to its requirements, including the requirement of complete and corresponding source code, unless it is specifically excepted. This principle often causes theoretical or speculative dispute among lawyers, because "the work" is not a unit of computer programming. In order to determine whether a "routine" an "object," a "function," a "library" or any other unit of software is part of one "work" when combined with other GPL'd code, we must ask a question that copyright law will not directly answer in the same technical terms. A lawyer's conclusion on that subject will be based on the application of rules made in the context of literary or artistic copyright to the different context of computer programming. The key here is that the GNU GPL licenses mean to "plow fence row to fence row," covering every version of "work based on the work" recognized by local copyright law, but no further.

The GNU GPL licenses express this scope by saying that their terms apply to the work as licensed, and to all works "based on the Program." GPLv2, a license made by US lawyers for US readers, says that

> "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.

This form of explanation was unfortunately unhelpful. It led to years of fruitless discussion about the role of "derivative works" doctrine (a US concept) in software (where US courts have largely failed to provide any guidance). So in GPLv3, we and our clients at the Free Software Foundation decided to drop all illustrative reference to US "derivative works," returning to the base concept only: GPL covers the licensed work and all works based on the work, where "based on the work" is defined as any modification or combination with the licensed work that requires copyright permission to make.

But the GNU GPL licenses recognize that what is outside their scope is as important to the protection of programmers' rights as their inclusive scope is important to the protection of users' rights. Where a programmer's work is "separate and independent" from any GPL'd program code with which it could be combined, then the obligations of copyleft do not extend to the work separately distributed. Far from attempting to extend copyleft beyond the scope of copyright, the licenses explicitly recognize, in the words of GPLv2 §2, that

> If identifiable sections of [other program code] are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License.

GPLv3 §5 goes further to protect the rights of programmers in such works from overextension of copyleft when it says that

> 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 individ-

> ual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

The GPL licenses, then, are explicit about limiting the scope of copyleft to the scope of copyright. They do not, however, as is sometimes suggested, do so in a way that distinguishes "dynamic" from "static" linking of program code in "early-binding" programming languages. It is occasionally suggested that a subroutine "dynamically" linked to GPL'd code is, by virtue of the linking alone, inherently outside the scope of copyleft on the main work. This is a misunderstanding. When two software components are joined together to make one work (whether a main and some library subroutines, two objects with their respective methods, or a program and a "plugin") the combination infringes the copyright on the components if the combination required copyright permission from the component copyright holders, and such permission was either not available or was available on terms that were not observed. Where a combination is made with GPL'd or AGPL'd components, the only available permission is copyleft, and its terms must be observed on the combination as a whole if the GPL'd component is to be used at all. Whether the combination is made with a linker before distribution of the executable, is made by the OS kernel in order to share libraries for execution efficiency at runtime, or results from "late-binding" of references in the language at runtime (as in Java programs) is irrelevant.[3]

Automatic Downstream Licensing

Each time you redistribute a GPL'd program, the recipient automatically receives a license, under the terms of the GPL involved, from every upstream licensor whose copyrighted material is present in the work you redistribute. You can think of this as creating a three-dimensional rather than linear flow of license rights. Every recipient of the work is "in privity," or is directly receiving a license from every licensor.

This mechanism of automatic downstream licensing is central to the working of copyleft. Every licensor independently grants licenses, and every licensor independently terminates the license on violation. In the case of GPLv2, this termination is automatic, while under GPLv3 the party breaching the

[3] It is important to note that LGPL may differ in its requirements for statically or dynamically linking modules with a covered work. This is explained in detail at page 37, below.

license's terms may be able to cure before termination. Parties further downstream from the infringing party remain licensed, so long as they don't themselves commit infringing actions. Their licenses come directly from all the upstream holders, and are not dependent on the license of the breaching party who distributed to them. For the same reason, an infringer who acquires another copy of the program has not thereby acquired any new license rights: once any upstream licensor of that program has terminated the license for breach of its terms, no new automatic license will issue to the recipient just by acquiring another copy.

Protection Against Additional Restrictions

Users' freedoms cannot be protected if parties can add restrictive terms to the copyleft. The "no additional restrictions" principle is therefore unwaivable if the GPL licenses are to achieve their primary objective. GPLv2 therefore requires that the *only* license terms available for works based on GPLv2 works are the terms of GPLv2. GPLv3, in §7, enumerates a few classes of permissible additional terms, to allow very limited license variations in particular circumstances. But with these exceptions, the "no further restrictions" principle applies strictly. For these reasons, acceptance requirements or ceremonies, including "click to accept" installation routines, violate the terms of GPL.

Imposition of Repugnant Terms

The principle of "no additional restrictions" deals with securing the copyleft against deliberate modification by one party in the sequence of sharing. But what if a party is under restrictions invisible to the license? If A has no legal right to pass to B all the rights in a program that he got from C, B will wind up with fewer rights than GPL seems to afford her, because the law will always conclude that A could not pass more rights than he had. The GNU GPL licenses resolve this difficulty in the interest of users' rights: if legal conditions imposed on you (by court order, or by your acceptance of legal restrictions in another instrument) prevent you from passing along all the rights contained in the GPL, you cannot distribute at all. The copyleft licenses do not allow for external legal conditions as an excuse for non-compliance with their terms.

This principle, against the "imposition of repugnant terms" is of importance with respect, for example, to patent licensing. If you accept a patent license that contains more restrictive terms than those of the relevant GNU GPL license, the repugnant terms in the patent license will prevent you from distributing the program altogether. It isn't the existence, or the assertion, of the patent claims themselves, or even the offering of a GPL-incompatible patent license that triggers the provision: only your acceptance of those terms, or a court order imposing them on you, can do so.

License Provisions Analyzed

From our discussion of *why* the GNU family of licenses requires some users and distributors of programs to take measures to protect users' freedoms downstream, we can now turn our attention to *what* those requirements are, and *how* to satisfy them. The following section describes, for each of the family of licenses, which provisions in the license text give rise to compliance obligations, with some specific suggestions for the most efficient means of discharging them. In the following section, we discuss more broadly how to achieve compliance through better software governance, and how to respond to compliance inquiries and complaints.[4] In practice, we have found that presenting this information in license-terms order yields a useful reference for lawyers.

GPLv2

Promulgated in 1991, GPLv2 is still after 23 years in service, the most widely used free software license of any type.[5] The Preamble of GPLv2, which primarily restates the social intentions of the licensor, also, along with Section 1 is the source of the requirement that the full license text must accompany every distribution of a source or binary version of each licensed work, to ensure that users have actual notice of their rights. This requirement is responsible for a surprisingly significant fraction of compliance complaints, primarily because users are not provided with required information about

[4] Most of the material presented here can be found in the authoritative and extremely useful "Frequently Asked Questions about the GNU Licenses" by the Free Software Foundation, available at `https://www.gnu.org/licenses/gpl-faq.html`.

[5] `http://www.blackducksoftware.com/resources/data/top-20-open-source-licenses`.

the presence of GPL'd programs and the applicable license terms in physical products that they have purchased. The most effective mode of compliance engineering is to treat the required license texts as a "make target" in the compiling, packaging and distribution of the software, so that license texts and other "collateral" for the software in a product stack are produced and verified at the same stages and in the same fashion that the binaries themselves are generated, tested and packaged. Businesses that SFLC has worked with around the world, including large multiform firms with many semi-independent business units making and distributing products containing GPL'd software have been able to achieve perfect compliance on these and similar points with fixes of this type.

The other compliance obligation arising from the frontmatter of GPLv2 is the obligation not to modify the license text itself. Occasionally compliance issues arise solely because a distributor has elected to remove words from GPL, or to add remedy or other "ancillary" provisions. Like the rest of the GNU family of licenses, GPLv2 is the copyrighted work of the Free Software Foundation, and only verbatim copying is allowed.

Section 1: Copying and Distributing Unmodified Versions of the Program

This section addresses the right to copy and distribute verbatim copies of the Program as you receive it and mandates the following:

- conspicuous publication of appropriate copyright notices;
- retention or addition of disclaimer of warranty, unless you are offering a warranty, which you may do;
- retention of all notices referring to GPLv2; and
- provision of a copy of the license.

Contrary to popular belief in the United States—where copyright notice was required for copyright protection until 1978—notice and registration are not required under the Berne Convention to secure copyright. In the US and most of the rest of the world, each developer holds copyright in his or her code the moment it is written. Notices, and—in the US—registration, do have some remaining legal effect, however. Addition and preservation of notices are required by almost every free software license. For detailed

discussion of best practices for maintaining copyright notices, see SFLC's "Managing Copyright Information within a Free Software Project."[6]

Section 2: Modifying the Program and Distributing the Modified Form

Section 2 is the heart of the copyleft in GPLv2. It directly implements the requirement that modified versions be distributed on the same license terms. The right of modification is one of the four basic rights, and GPLv2 therefore protects rather than restricting its exercise. But as section 2 states, any modified version of a GPL'd program is *ipso facto* a "work based on the Program," and can only be distributed to others on the terms contained in GPLv2 and on no other terms.

Section 2(a) requires that all modified versions be so marked, with basic indication of the modifications made, the date of modification, and some identification of the modifier. Compliance is achieved by any markings in source code that contain this information in a reasonable form. Not all the information available from a source code version control system need be provided, nor is the requirement a substitute of the project-level ChangeLog or similar file. Appropriate compliance assists a programmer using or reviewing any particular source file to know from what version of a project or program that source file comes, and to trace the history of recent substantive modification.

In addition, as a further protection for others' legal notices, section 2(c) provides that if the program before modification "normally reads commands interactively when run" and displays or prints legal information, all copyright notices, warranty disclaimer, modification indications and a pointer to the license text must be displayed or printed in interactive use. For example, the GNU Debugger, gdb, or GNU zile.

GPLv2 §2 is as much about what copyleft does *not* require, as about the requirements themselves. The remaining three paragraphs of §2 limit the scope of copyleft in both intention and operation. Section 2 makes clear that GPLv2 does *not* purport to extend copyleft to code written entirely by non-licensing authors who have made separate and independent works that *could* be usefully combined with GPL'd software. So long as those separate,

[6] `http://softwarefreedom.org/resources/2012/ManagingCopyrightInformation.html`.

independent works are delivered separately, or even are only "aggregated" with GPL'd programs on a medium of software distribution like a DVD or a USB stick, the license specifically disclaims any copyleft obligations on that code. Only when a new "work based on the Program" is created by combining this previously-separate work with GPL'd code, or when the work is not really independent because it cannot execute unless combined with GPL'd code, does the copyleft obligation attach to the new work so created.[7] In the aggregation case, the license makes clear, the aggregate cannot be released under an umbrella license that prohibits users from exercising rights that each program's individual license grants them.

Section 3: Copying and Distributing a Program in Object Code Form, Modified or Unmodified

GPLv2 §3 sets the terms for distribution of executable or binary versions of the work. Though §2 is the heart of the copyleft, §3 is the source of the most important compliance obligations. Users cannot study, understand , modify and share programs without buildable source code, which is therefore what §3 requires they be offered. There are three primary forms of compliance with §3:

1. When executable copies of GPL'd programs are available for copying over the Net, complete and corresponding source code may be made available for copying from the "same" place;
2. When executable copies of GPL'd programs are distributed on physical media, they can be accompanied by source code on the same media, or on other units in a collections of, e.g. DVDs or USB memory sticks;
3. Executables distributed in these and other ways may be accompanied by a written offer, valid for at least three years, for complete and corresponding source code. If you are a non-profit redistributor casually redistributing someone else's packaging of GPL'd code, which was accompanied by written offer rather than source code, you may pass

[7] This covers the full scope of primary infringement liability for non-compliance. Secondary copyright liability may attach in other ways. If, for example, I create a proprietary enhancement to a GPL'd work and deliver it separately, advertising its availability and encouraging downstream users to make and redistribute the infringing combination of my proprietary enhancement and the original GPL'd work, once such an act of primary infringement has occurred, the GPL-licensing copyright holders can and will succeed in claims for inducing and contributing to copyright infringement against me. See MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

> along the written offer you received. For an example of a compliant written offer for source code, see Appendix I.

What constitutes "complete and corresponding source code"? In the first place, source code is "the preferred form for making modifications to the work." For interpreted computer languages, from shell script to Perl to Javascript to APL, the preferred form for making modifications may well be the only form of the program. (Attention should be paid, however, to compression, minimization, obfuscation, and other modifications to interpreted code that may result in the creation of a "non-source form.")

Complete, and as §3 says, "corresponding" source means the source code, build scripts, makefiles, configuration files and other materials necessary to build a version of the program precisely equivalent to the executable delivered, to modify that source code, and to build the modified version. Lacking anything necessary to build the precise version delivered means the source distributed is incomplete and not "corresponding." "Corresponding" source code unsuitable for modification and rebuilding into modified versions, as for example because too heavily obfuscated to be practicably modifiable, would not be "complete."

The completeness requirement contains an exception for system libraries, defined by §3 as:

> 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.

The goal of this exception is to relieve distributors of the requirement to deliver source code that the downstream user does not require in order to exercise her rights, because that code is available as part of the operating environment the user can be presumed to have already available to her.

Failure to provide or offer complete and corresponding source code is the single largest failure mode leading to compliance disputes. All the litigated cases of community complaint against commercial redistributors involved failure to provide complete and corresponding source on valid request. Verification that source code provided in response to compliance request is in fact complete and corresponding is the single most burdensome and difficult part of compliance enforcement. All these problems result from inadequate governance. Parties do not retain the source code of binaries embedded in their products. They lose the human resources that knew how to build

their software components. When, at some later time, copyright holders whose works have been modified and redistributed seek the source code, organizations don't know how to provide it, or provide radically incomplete or inadequate code, and reflect helplessness and ignorance as though either constituted legal excuse.

None of this should or need happen. If the tarball of complete and corresponding source code is also a "build target" in the software production process, so that no binary build is successful unless complete and corresponding source code has also been produced, no source code can be lost. So long as the component can be built, the engineering knowledge to build it cannot leave the firm. Provisioning of public-facing source code on the Web can be an automated part of product shipment or release to manufacturing. In our work with firms around the world, we have repeatedly found that relatively simple and completely inexpensive changes to software development practices could entirely eliminate modes of compliance failure that elude the scrutiny of "compliance tools" costing orders of magnitude more.

Use of a written offer for source code may time-shift your obligation to provide source code but it also increases your compliance costs in the long run. Your offer must be good for at least three years even if you have stopped distributing your product. This also makes it possible for "any party" to demand a copy of complete and corresponding source code, even if the requester has not received a binary.

If you are a commercial distributor of GPL'd program, even if you merely redistribute software produced by someone else, you are bound by the terms of the GPL. In such cases it is never sufficient to merely pass along the same written offer for source that you received from your upstream licensor or supplier and expect your users to get the source code from your supplier. In such instances it is advisable that you exercise your own rights as a user to request C&CS for all the GPL programs that your suppliers provided to you, preferably in an automated process. Once you receive such C&CS, passing it along with your product will ensure your compliance with the license.

The equivalent provision in GPLv3 is Section 6 that deals with conveyance of source code in non-source forms.

Section 4

Section 4 expresses the "no additional restrictions" concept directly. It also prohibits sublicensing on non-GPLv2 terms. This prohibition bears notice.

It is conventional, but incorrect, to state that copyleft obligations apply only when GPL'd code is distributed. Sublicensing is a separate activity that also gives rise to copyleft obligations.

Until the second decade of this century, the possibility of noncompliance with GPLv2 through sublicensing was a rare, near theoretical occurrence. No longer. "Cloud" offerings of "software as a service," in which virtualized server stacks are sold on a utility-computing basis have brought about significant noncompliance. Firms offering such virtualized server instances often enter contracts with their users purporting to "license" the software in their virtualized server stacks, which will almost always include GPL'd OS components being thereby sublicensed on incompatible terms. Efforts to avoid this outcome require no technical or engineering measures.

GPLv3 prohibits sublicensing altogether, see page 20 below. "Cloud" or "software as a service" deployments of GPLv3 software can therefore also be technically fully compliant but infringing as a result of mistaken contracting.

Section 4 of GPLv2 provides that license termination is automatic in the event of violation of terms. This rule was changed in GPLv3 §8, see page 26 below. Because license termination automatically occurs on infringement, resumption of distribution (which can be automatic under GPLv3) requires an affirmative regrant of the right to distribute from the copyright holder. Although community copyright holders have been uniformly cooperative with requests by former infringers to resume distribution upon rectification of rights, it is the inevitable consequence of more concentration of GPLv2 copyrights in for-profit organizations engaged in monetizing their copyrights that there will be future cases in which automatic termination results in substantial monetary demands for reinstitution of rights. Because automatic termination leads immediately to injunction a non-community monetizing GPLv2 copyright holder gains potentially unfair leverage from automatic termination. This is among the most important reasons why commercial redistributors should now prefer GPLv3 to GPLv2 terms from their upstream technology providers.

Section 5: Acceptance of License Not Required

The English common law tradition has defined "license" for more than 500 years as a unilateral permission to use property rights granted by the owner to non-possessors. In the traditional law school property course, the example

of a license is an invitation to dinner. If I invite you to my house for dinner, and sue you for trespass when you cross the threshold, your defense is "license," a unilateral permission to be there. Confusion about the status of licenses as contracts is endemic in global legal analysis, because in many other legal systems, including those claiming descent from Roman law, the idea of non-contractual unilateral obligation is unrecognized. (Though you still can't sue someone for going where invited.) The GNU licenses are licenses in the common law sense: unilateral copyright permissions within limits. GPLv2 §5 states this frequently-controverted but unassailable legal distinction. Acceptance of the license is not required, nor is it sought. A requirement of acceptance, through clickwrap or other ceremonies, is not only not required, it is an imposition of additional conditions forbidden by the terms of the permission granted in the license. Compliance with §§4 and 5 therefore requires the explicit avoidance of contractual forms, acceptance ceremonies, monitored assent, or any other activity designed to turn unilateral permission into bilateral obligation.

Section 6: Automatic Downstream Licensing

This is GPLv2's "automatic downstream licensing" provision. Each time you redistribute a GPL'd program, the recipient automatically receives a license from each original licensor to copy, distribute or modify the program subject to the conditions of the license. There is no requirement to take any action to ensure the downstream recipient's acceptance of the license terms, see above. This places every copyright holder in the chain of descent of the code in legal privity, or direct relationship, with every downstream redistributor. Two legal effects follow. First, as §6 says, parties themselves remaining in compliance have valid permissions for all actions including modification and redistribution even if their immediate upstream supplier of the software has been terminated for license violation. Their licensed rights are not dependent on compliance of their upstream, because their licenses issue directly from the copyright holder. Second, automatic termination cannot be cured by obtaining additional copies from an alternate supplier: the license permissions emanate only from the original licensors, and if they have automatically terminated permission, no act by any intermediate license holder can restore those terminated rights.

It also follows, as §6 makes clear, that licensors are in no way responsible for enforcing compliance by third party recipients or distributors. Every

licensee gains or loses permissions from each original licensor solely on the basis of its own conduct.

Section 7

This provision deals with the problem of the licensor who is prevented from passing on the freedoms guaranteed by the license due to interfering obligations. Compliance with §7 means if conditions are imposed upon you that conflict with the requirements of the license, you cannot and must not use the license to redistribute others' code. Unless the copyright holders have provided you with additional permissions, therefore, if you are under exogenous legal obligations you may not redistribute the program or works based on the program at all.

The term "conditions imposed on you" is crucial to the interpretation of GPLv2 section 7 in this regard. Conditions are "imposed" if a court or another settlement agreement you may have entered into has imposed them. So a compulsory license or a court-ordered settlement which contains provisions requiring, e.g. per-unit royalties or bars downstream resale would trigger §7 obligations. Accepting a patent license, or entering into any other contract restrictive of rights has the same effect.

Compliance with GPLv2 §7 is therefore a matter of legal review rather than technical or engineering practice. To our knowledge, no litigation or adversary proceedings have been brought by community organizations for breach of §7 in the past, but in our practice we have more than occasionally discussed with firms whether particular arrangements they had entered into should be nullified or modified to avoid §7 problems.

The other crucial function performed by GPLv2 section 7 is the function of discouraging separate settlements in patent disputes. A settlement allowing only the settling party to distribute GPL'd software with patent safety cannot be an effective limit unless it prohibits redistribution by downstream parties. If it does so, however, it constrains the rights being transferred by GPL, and falls foul of §7.

GPLv3

Promulgated in 2007 after eighteen months of public discussion, GPLv3 adds some additional compliance obligations under certain circumstances, but

also makes central compliance obligations easier to fulfill, and substantially removes the risk of automatic termination for unintentional infringement.

The drafting principles adopted in GPLv3 took as their principal aspiration the avoidance of US-specific or system-specific vocabulary, in order to avoid importation of system-specific legal assumptions. The words "distribution" and "derivative work" in GPLv2, for example, caused analytical confusion for little overall benefit. With the immense expansion of use of GPL'd software around world since 1991, FSF and its lawyers here decided to avoid system specific language to remedy that risk of confusion.

Two terms are used in GPLv3 deliberately exotic to the language of international copyright. To "propagate" a work covered by the license means any activity that requires permission of copyright holders in the local legal system where the activities are carried on. Personal use or modification for personal use are activities explicitly excluded from "propagation" regardless of domestic copyright law, in order to prevent domestic copyright law from trenching on freedoms 0 to 2. As a further benefit, because "propagation" includes all exclusive rights granted under any particular copyright regime, regimes that require a valid license to account for all exclusive rights are automatically complied with.

Any propagation that enables other parties to receive or make copies of the work, is called "conveying." In general, conveying is the activity that triggers copyleft obligations. Explicitly exempted from "conveying" is "interaction with a user through a computer network, with no transfer of a copy," which distinguishes GPLv3 from AGPLv3, see page 33 below.

Use of these terms allows GPLv3 to be interpreted authoritatively based solely on local legal knowledge and the technical facts. Parties who may have questions about compliance with GPLv3 under domestic copyright provisions need only to ask two questions, one legal and the other factual:

1. Do I need a license under local copyright law to carry out this activity?
2. Does my activity enable any other party to make or receive a copy of the program?

If question 1 is answered by a local copyright lawyer in the negative, then the activity involved is not propagation and is permitted by GPLv3 without more. If the answers to both questions are positive, then the activity involved is "conveying," and copyleft obligations imposed by §§4-6, below, apply.

GPLv3 requires the conveyors of the work to provide all the source necessary to build the program, including supporting libraries, compilation scripts, etc. "Corresponding Source" in GPLv3 §1 is defined as:

> [A]ll the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

Both versions of GPL except from the requirement to produce complete and corresponding source code the source code for "System Libraries", commonly called "the system library exception." As can be seen in the quotation above, the intention of the "System Library exception" is to avoid the need for production of source code which the user can expect to receive with the copy of the operating system, to the extent source code for the operating system is available at all, or of the generally-available programming tools used to produce the program.

Section 2: Basic Permissions

The license explicitly affirms your unlimited permission to run the unmodified program. You can only make modifications, or otherwise propagate a covered work, even one that you do not convey, so long as you are in compliance with the license terms. If your license is terminated, then, for example, you cannot continue to service your copies by making new modified versions.

Section 2 clearly states that sub-licensing under the terms of the license is not allowed. As we have previously noted, incautious contract drafting in "software as a service" or other cloudy contexts can fall, and has fallen, foul of this prohibition.

Section 4: Conveying Verbatim Copies

Under §4 anyone may convey without limit verbatim copies of program source code. The conveyor's compliance obligation is limited to the curation of copyright notices and the provision of the license text along with the source code. If copyright notices are missing, they must be added. All notices of attribution and additional permission pursuant to §7 below must be preserved (or added in the case of new attributions and permissions), and all upstream disclaimers of warranty must be preserved. Automated software governance processes are sufficient to meet all §4 obligations simply and cheaply.

Section 5: Conveying Modified Source Versions

Notice obligations under §5 are identical to those under §4, with the additional requirement to provide notice of modification, date and some identification of modifier as under GPLv2 §2(a), above.

§5 also restates the aggregation provision of GPLv2 §2, as follows:

> 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.

Section 6: Conveying Non-Source Forms

Section 6 states the compliance obligations for distributing "non-source forms" of a program, which means any form other than the form preferred for making modifications. In addition to binaries or executables, non-source forms therefore include obfuscated, minimized, compressed or otherwise non-preferred forms for modification. Non-compliance with GPLv3 in the distribution of Javascript on the Web is becoming more frequent, and although

no disputes have so far resulted, in the absence of more careful compliance activity in this area they are eminently foreseeable.

The requirement to provide complete and corresponding source code under §6 closely parallels the provisions of GPLv2 §3, above, but with changes designed to make compliant provisioning easier under contemporary technological conditions. Source code may be provided by online distribution as under GPLv2, but the "same place" requirement of GPLv2 §3 is loosened slightly:

> If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

This provision allows, for the first time, for third-party provision of complete and corresponding source code in commercial distribution situations. The obligation remains on the party distributing the non-source form to point prominently ("next to" the non-source download) to the third-party source code provisioning server, and to ensure that this third-party server remains in operation for required period.

Section 6 also allows the provision of source via such a server when the binary or other non-source form is distributed by peer-to-peer protocols such as BitTorrent. Here the requirement is only that each peer be effectively informed of the location of the source code on a server as above.

Section 6 slightly modifies the rules pertaining to written offers. Under GPLv2 §3(b) above, written offers must be valid for a period of three years. GPLv3 §6 requires that the period of validity of the offer be the longer of three years and valid for the period for which other spare parts and/or customer service are available for any physical product embedding the program.

The definition of "system libraries" in the exception from corresponding source code in §1 substantially varies from the parallel definition in GPLv2 already discussed. The new definition says:

> The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal

> form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

This definition clarifies that language processors (compilers and interpreters) included in the distribution of the program's target operating system are not part of the corresponding source. As in GPLv2, libraries or other enabling or ancillary code accompanying major components of the operating system are excepted as well, as is any code providing an implementation of a publicly documented "Standard Interface" for which a source code version of an implementation is publicly available.

The most widely-discussed new requirement in GPLv3 is also found in §6: the requirement to provide "installation information" for GPLv3 code in "user products." The intention of the "installation information" provision of §6 is to protect the rights of users to modify and run modified versions of GPLv3 code embedded in products that they own and personally use. Without such a provision, "lockdown" of devices to prevent modification of software by legal owners could vitiate the freedoms GPL-licensing authors intend their users to have. If all embedded devices implemented such lockdown, the freedoms guaranteed by GPL would become, as the US Supreme Court once said, "a promise to the ear to be broken to the hope . . . ." *Edwards* v. *California,* 314 U.S. 160, 186 (1941) (Jackson, J. concurring).

A "user product" is

> either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling.

When non-source forms of a GPL'd program are conveyed to a user embedded in a "user product" by permanent transfer of ownership or control of the device, or by lending or rental for a fixed term, the corresponding source must be supplemented by sufficient technical information

> methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made

Unless technical measures have been employed in the device to prevent the installation and execution of modified versions, this requirement is trivial. Experience since 2007 has tended to show that manufacturers who intend to lock down their consumer products therefore avoid GPLv3 software. No adversary actions over non-compliance with the installation information requirement have occurred to our knowledge since the promulgation of GPLv3.

Section 7: Additional Terms

While GPLv2 does not allow for any additional restrictive terms, GPLv3 allows for some specific limited variations, thus varying the strict copyleft of GPLv2 in the interest of broader compatibility with other licenses. Section 7 consists of additional permissive and non-permissive terms which can be used to supplement the terms of the License. Additional permissions beyond those of §7 can be placed by any copyright holder on her contributions to a licensed work. GPLv3 states, as GPLv2 does not, that all additional permissions must be in writing. In the drafters' view, the granting of informal or unwritten additional permissions under GPLv2 created unnecessary doubt. Written additional permissions previously granted by upstream authors can be removed before conveyance of a copy of the Program if so desired by the conveying party.

Section 7(a) – Disclaimer of warranty: Copyright holders can disclaim warranty or limit liability differently from the terms as provided under §§15 & 16. Internationalization of GPL required the drafters to permit the variation in such terms necessary to deal with the absence of any international harmonization of the laws of warranty and disclaimer.

Section 7(b) – Preservation of appropriate legal notices. Section 7 permits additional terms requiring preservation of legal notices, including on output from execution of covered works.

Section 7(c) – This provision allows for prohibition of misrepresentation of original material and makes GPLv3 compatible with permissive licenses that require modified versions be marked in "reasonable" ways which are different from the precise marking requirements of GPL itself.

Section 7(d) – Limiting the use of names of licensor for publicity purposes. This provision was added to provide compatibility with licenses which prohibit the use of the licensor's name on unmodified versions and other prohibitions on advertising rights. The long-standing and occasionally troublesome incompatibility with the "BSD advertising clause" is an example of the friction removed by this provision.

Section 7(e) – No grant of rights under Trademark Law. This provision serves a similar function with respect to "no trademark grant" clauses in permissive licenses.

Section 7(f) – allows for requiring of Indemnification of authors and licensors, removing one of two primary sources of incompatibility with the Apache Software License version 2.0.

Any other non-permissive additional terms apart from those stated above are considered "further" restrictions and are prohibited by §10. If you add any kind of additional terms in accordance with §7, you must ensure that the terms are placed in the relevant source files or provide a conspicuous notice about where to find the additional terms. Compliance obligations as presented by §7 are entirely a matter of legal review, without technical or engineering consequences.

Example: GNU Compiler Collection (GCC) Runtime Library Exception This GCC Runtime Library Exception ("Exception") is an additional permission as provided by Section 7 of GPLv3. The purpose of this Exception is to allow compilation of non-GPL (including proprietary) programs making use of the header files and runtime libraries covered by this Exception and containing code from the copyleft toolchain embedded by the compiler in the object code of the program as part of the compilation process. The GCC Runtime Library Exception covers any file that has a notice in its license headers stating that the exception applies. This includes libgcc, libstdc++, libfortran, libgomp, libdecnumber, libgcov, and other libraries distributed with GCC.

Section 8: Termination

The change from automatic termination on violation to a period for self-cure and automatic reinstatement of rights for first-time violators is one of the most important modifications of the basic rules of compliance enforcement from GPLv2 to GPLv3.

> However, if [after your discovery of a breach of the license terms] you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.
>
> Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

The realignment of incentives to find and fix problems is a major advantage of GPLv3 over GPLv2. Automatic termination requiring positive reinstatement by copyright holders to avoid loss of distribution rights created incentive to hide problems rather than fixing them. Cases of "whole distribution infringement," that is, failure to provide corresponding source code for all the copylefted programs in an entire OS distribution embedded in a device, result in the infringement of hundreds or thousands of copyrights at once. This situation poses immense obstacles to successful remediation by violators, who may without restoration of rights be unable to distribute their products. In one recent matter, we were retained to audit a medium-sized business relatively inexperienced in compliance engineering. We found that a "whole distribution infringement" situation in past products required them to contact all the copyright holders in more than 100 packages licensed under GPLv2, in order to assure their right to continued distribution of new models of products built compliantly, because their previous non-compliant distribution of the same programs in earlier products led to undiscovered automatic termination.

Section 10: Automatic Licensing of Downstream Recipients

This Section manifests the no-additional restrictions and automatic downstream licensing principles as discussed in other parts of this document. Enforcing your patent claims against those to whom you distribute a program constitutes an additional restriction and is prohibited by Section 10

Mergers and Acquisitions Section 10 also clarifies that in business acquisitions, whether by sale of assets or transfers of control, the acquiring party is downstream from the party acquired. This results in new automatic downstream licenses from upstream copyright holders, licenses to all modifications made by the acquired business, and rights to source code provisioning for the now-downstream purchaser.

In our experience, the process whereby these matters are adjusted in most M&A situations are ludicrously expensive and inefficient. A simple waiver and release of all claims to GPL compliance against the purchased entity by the purchaser, issued before closure, removes the problem. If the purchasing entity has adequate software governance systems in place, all software acquired in the course of the entity transaction is input to the standard governance processes for acquired software, and downstream compliance by the new merged entity is automatically handled.

Section 11: Patents

GPLv3 provides for two classes of patent commitments:

1. Prohibition of Enforcement of patent claims against those to whom you distribute: GPLv3 §10 makes explicit that demands for acceptance of patent licenses or payment of patent royalties by those to whom a licensee directly distributes are additional conditions that may not imposed. This provision establishes a uniform rule of patent exhaustion with respect to GPL'd programs regardless of the domestic patent law in any particular system or locale.

2. Grant of license to claims in contributor versions: Section 11 introduces an affirmative grant of rights to patent claims by those who contribute code to GPL'd programs. The intent is to prevent parties within the commons from aggressively asserting patents against

> users of code they have themselves modified, preventing a form of commons betrayal by "insiders" to the community. A contributor's patent claims necessarily infringed by the version of the program created by the incorporation of its modifications are licensed to all subsequent users and modifiers of the program, or programs based on the program. No patent claims only infringed by subsequent modifications by other parties are thus licensed. Patent claims acquired after the making of the "contributor version" necessarily infringed by that version are also licensed by this provision at the time of their acquisition or perfection. When a company with a large number of such claims acquires the program's modifier, all claims held or thereafter acquired by the purchaser are automatically licensed under this provision. The acquisition of Nokia by Microsoft, for example, resulted in the automatic licensing of all Microsoft claims now or hereafter acquired which read on any contributor version of any GPLv3 program ever modified by Nokia. The wholesale decimation of Microsoft patent claims on GPLv3 programs arising from the purchase of Nokia has so far been unremarked in the industry.

Section 11 also deals with the possible efforts to undermine common rights in GPL'd code by parties colluding to enforce discriminatory patent licenses. If A takes a patent license from B that benefits A only, rather than A's customers or their distributees, A imposes risk from B's patents on others that it does not suffer itself. Under many circumstances, this is an acceptable outcome. If, however, A is the only possible source of the program, by taking such a license and distributing in reliance on it, A is in effect helping B to "take the program private." Section 11 poses several possible solutions A could undertake, including disclaiming the license or securing its extension to all parties. But the most likely compliant action, and the least costly, is simply to ensure that the program source code is available permanently through some third party, so that those who wish to develop or commercially deploy or redistribute the code at their own risk can do so.

In addition to this "downstream shielding" provision, §11 takes two other steps to avoid exploitive manipulation of discriminatory patent licensing tactics:

> If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate,

> modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

If, for example, company B offers purchases from company A a number of coupons entitling third parties to the GPL'd programs distributed by A, and provides access to its patent claims reading on those programs only to those acquiring A's product through purchase or gift of the coupons from B, this provision deprives B of its value in the transaction by automatically extending the patent license to all other users. Experience suggests that B will retroactively assert that the coupons thus issued did not apply to any GPLv3 programs in the collection of software covered by the coupons. This won't work.

> A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

This provision was adopted in order to prevent the spread of a particular transaction type entered into between two firms during the public discussion process conducted by the Free Software Foundation leading to the adoption of GPLv3. There are no current compliance issues related to this provision, so far as we are aware.

Patent Assertion & Retaliation: GPLv3 implements a narrow scheme of patent retaliation against those who undertake patent aggression against licensed works which they distribute or contribute to. Read together, §§8, 10 and 11 establish defensive patent suspension and termination conditions.

The termination provision of section 8 states that if a licensee violates the terms of the GPL, a contributor may terminate any patent licenses that it granted under §11 to that licensee, in addition to any copyright permissions the contributor granted to the licensee. Therefore, a contributor may terminate the patent licenses it granted to a downstream licensee who brings patent infringement litigation in violation of §10.

Section 12: No Surrender of Others' Freedom

GPLv3 §12 is functionally identical to GPLv2 §7. An illustration in the GPLv2 provision caused more confusion than it was worth, and has been omitted. In all other respects, including in their compliance consequences, the provisions have the same effect. See page 18 above.

Section 13: Use with the GNU Affero General Public License

This section specifically gives permission to link or combine any work that is licensed under GPLv3 with a work licensed under AGPLv3. The compliance consequences of this permission are discussed with respect to the AGPLv3, below.

The resultant work will be governed by the terms of GPLv3 but if the work is used over a network then the terms of AGPLv3 shall apply to the entire work.

You cannot take code released under the GNU AGPL and convey or modify it however you like under the terms of GPLv3, or vice versa. However, you are allowed to combine separate modules or source files released under both of those licenses in a single project.

When a combined work is made by linking GPLv3-covered code with AGPL-covered code, the copyleft on one part will not extend to the other part. That is to say, in such combinations, the Affero requirement will apply only to the part that was brought into the combination under the Affero license. Those who receive such a combination and do not wish to use code under the Affero requirement may remove the Affero-covered portion of the combination.

GPL Special Exception Licenses

GNU Classpath & GPL Linking Exception

GNU Classpath is the GPL-licensed set of essential libraries for the Java programming language. It is licensed under the GPL plus a special exception:

> Linking this library statically or dynamically with other modules is making a combined work based on this library. Thus, the terms and conditions of the GNU General Public License cover the whole combination.
>
> As a special exception, the copyright holders of this library give you permission to link this library with independent modules to produce an executable, regardless of the license terms of these independent modules, and to copy and distribute the resulting executable under terms of your choice, provided that you also meet, for each linked independent module, the terms and conditions of the license of that module. An independent module is a module which is not derived from or based on this library. If you modify this library, you may extend this exception to your version of the library, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version.

AGPL

Whether to extend the copyleft concept to the delivery of services by free software over a network is a complex issue long discussed in the free software community. Freedom zero requires that any user be allowed to run any program for any purpose, which of course includes the provision of computing services to others. Freedom two requires respect for the right of private modification. Their combination requires that anyone be able to run privately-modified copies of GPL'd programs for the purpose of providing computing services to others.

But there are good reasons why programmers developing software for use in network services provision, particularly the infrastructure of Web applications, would want to require that parties offering services using modified

versions of free software allow their users the same rights offered to those modifiers by the original developers. Federated or "free" services platforms benefit from this licensing model.

Rather than resolving the conflict within the scope of one license, the Free Software Foundation experimented over an extended period with licenses for such "copylefted services" software that could be made partially compatible with GNU GPL. Two such licenses, AGPLv1 and AGPLv3, different in their architecture but similar in their intention, have been published and used.[8] The "A" in AGPL standards for "Affero," the name of a software project pioneered by Henry Poole, a director of FSF. AGPLv1 was written by FSF specifically for use by Affero, and was published in 2003. AGPLv3 was designed and drafted in parallel with GPLv3, to unify more closely the relation among these licenses, and to permit use of GPLv3-licensed code in AGPLv3-licensed projects.

The common architectural feature of the AGPL licenses is a separate "trigger" condition, in addition to the triggering conditions for copyleft obligations ("distribution" and sublicensing established by GPLv2) and "conveying" established by GPLv3. The *scope* of copyleft under the AGPL licenses is the same as the scope of copyleft under the respective version of GPL. Only the condition that gives rise to the obligations to provide corresponding source code and license texts are changed.

AGPLv1

AGPLv1 is GPLv2 with a single additional requirement, found in §2(d):

> If the Program as you received it is intended to interact with users through a computer network and if, in the version you received, any user interacting with the Program was given the opportunity to request transmission to that user of the Program's complete source code, you must not remove that facility from your modified version of the Program or work based on the Program, and must offer an equivalent opportunity for all users interacting with your Program through a computer network to request immediate transmission by HTTP of the complete source code of your modified version or other derivative work.

[8] AGPLv2, published in 2007, is a transitional license "stub" permitting any licensee to distribute works based on AGPLv1 programs under the terms of AGPLv3.

This requirement, parallel to the "preservation of notices in interactive use" requirement of GPLv2 §2(c) was invented by Bradley Kuhn when he was Executive Director of the Free Software Foundation. Compliance with its requirement was straightforward: if the feature to request server-side source code was present in a program "intended to interact with users through a computer network," compliance consisted of not removing it.

AGPLv3

AGPLv3 is GPLv3 with one additional requirement, contained in AGPLv3 §13. Like AGPLv1, AGPLv3 makes no modification whatever to the scope of copyleft. In deciding what source code is the "corresponding source" to be provided or offered under AGPLv3 §6, it is sufficient to ask what source code would have to be provided if the same program were delivered to its user in a non-source version on a medium of physical distribution.

The additional triggering condition of AGPLv3 is as follows:

> if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

Compliance requires that any version of the program that you yourself modify, and which retains the architecture of interacting with its users remotely over the network, must afford the user an opportunity to receive corresponding server-side source code over the network. If a corresponding source archive is itself a "make target" in the process of building the program, as we suggest with respect to all copylefted works, then the implementation of the compliant feature for early-binding languages is as simple as outputting that source archive (and possibly other source archives from other running programs that are part of the same system) into the communication stream as constant data when the running program receives the relevant request. This technical approach to compliance also resolves "scope of copyleft" issues

for programs written in early-binding compiled languages: if components of the program as run are determined at make time, then what it took to make the program, minus the system libraries and any other excepted code, is the corresponding source.

Taken together, GPLv3 §13 and AGPLv3 §13 ¶2 establish the compatibility structure for combining GPLv3- and AGPLv3-licensed code. GPLv3 gives permission for code under its terms to be combined with code under AGPLv3's terms, each part to be treated as under the terms of its respective license. AGPLv3 code cannot be relicensed under GPLv3, or the reverse, without additional permission from the respective copyright holder. Source code licensed under GPLv3 is part of the corresponding source of any work combining code under the two licenses.

LGPL

The Lesser General Public License, whose terms apply to the GNU C Library, among other works, is sometimes described as a "weak copyleft" license, because code licensed under LGPL's terms can be combined with code under non-free licenses, and is sometimes used in that fashion. But, although the two versions of LGPL currently in use differ very substantially in their content and architecture, they are instead both strong copyleft licenses with broad linking exceptions. Understanding how to comply with the licenses hinges on this often-misunderstood distinction. LGPL'd code is never placed under new or alternative terms when it is combined with code under non-copyleft licenses. The combination is permitted, but the LGPL'd components of the program remain under the terms chosen for them by their copyright holders. This is not closely analogous to the behavior of licenses like the Eclipse license that, at the file level, assures source code is distributed under copyleft terms, while binaries may be distributed under any terms at the redistributor's discretion. LGPL's versions are intended to assure downstream users' rights in that potion of the permitted combination which consists of LGPL'd code, in both source and non-source forms.

LGPLv2.1

LGPLv2.1 is a copyleft license in its own right, to which §6 is an exception permitting non-copyleft combinations. The analytical peculiarity is that the copyleft license from which LGPLv2.1 §6 is an exception is not GPL. It is

LGPLv2.1 §§1-5, which does not behave in all respects like any version of GPL.

Section 0: Definitions and Scope of License Section 0 of LGPLv2.1 states that translation "straightforwardly" into another programming language of an LGPL'd program or library of routines is the creation of a modified version of the licensed program. GNU GPLv2 and GNU GPLv3 do not contain this definition.

Section 2 Section 2(a) states that if a licensed work is a software library (defined in §0 as "a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables") permission is given to distribute modified versions only if those versions are themselves libraries. LGPLv2.1 code can therefore *not* be compliantly taken from its context in a library and placed in a non-library modified version or work based on the work. Section 6 does not provide an exception for this rule: a combination may be made of a modified version of an LGPL'd library with other code, but the LGPL'd code must continue to be structured as a library, and to that library the terms of the license continue to apply.

Section 2(d) states that modified versions of library routines must not require non-argument global data unrelated to library function in order for library functionality to work. This means that libraries may not be modified to require keys, tokens, tables or other non-functional restrictive data to be present in order for applications to call and receive services from routines in the library. Section 6 does not except from these requirements. Compliance requires avoidance of such schemes, which in the years since LGPLv2.1 was promulgated in 1999 have become relatively common.

These requirements of §2 are stringent, and standing alone they would trench too closely on users' freedoms. But LGPLv2.1 §3 allows all works under its terms, copy by copy, to be used instead under the terms of GPLv2 or any later version. This provides a pathway for those who do not want to use code under the requirements of LGPLv2.1 to do so under GPLv2 or GPLv3 at their discretion.

Section 6 of the license contains a functional anti-lockdown provision, requiring that any LGPL'd code provided to the user as part of such a proprietary

or non-copyleft work must permit relinking or re-installation of a modified version of the library.

Section 2 repeats, as in GPLv2, that

> These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Given the context of §2, it is apparent that this clause is not to be read as limiting in any way the exception for combinations under §6. But with respect to modified versions of the LGPL'd work itself, this language in §2 reaffirms that §6 is inapplicable.

Section 4 Section 4 covers distribution of non-source forms of unmodified versions of covered works, or works modified as permitted by §2. Compliance with its provisions is as for compliance with the parallel provisions of GPLv2, above.

Section 5 Section 5 addresses directly the ambiguities arising from the application of copyright law to software:

> A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.
>
> However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

> When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

Accordingly, with the intention of avoiding situations in which such ambiguity may arise, §5 goes on to state:

> If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)
>
> Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

Here, the clear purpose of the provision is to waive copyleft in ambiguous situations to the extent of permitting combinations under the exception provided in §6. To our knowledge, no public action of enforcement of LGPLv2.1 in the area delineated by Section 5 has ever occurred.

Section 6 §6 provides the combination exception that is often misunderstood as a "weak copyleft" license, which it is not. It permits combinations of the licensed work or works based on it

> to produce a work containing portions of the Library, and [to] distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

These requirements on the licensed combination require that the license chosen not prohibit the customer's modification and reverse engineering for debugging these modifications in the work as a whole. In practice, enforcement history suggests, it means that the license terms chosen may not prohibit modification and reverse engineering for debugging of modification in the LGPL'd code included in the combination.

§6 also requires that:

> You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License.

This is not identical to the roughly parallel requirements of GPLv2 and GPLv3. Compliance requires slightly different measures with respect to the "credits" or "licenses" or "about" screens in interactive programs.

In addition, §6 requires either that source code be provided or offered for the LGPL'd portion of the combined work, or that a "shared library" mechanism be used that allows dynamic replacement of the licensed work by modified versions.

If source code is provided, §6(a) states requirements that vary from those of GPLv2 and GPLv3:

> [You must] Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Not only must the source code be complete and corresponding, but it must be provided in such a way that a modified version of the entire combined work can be regenerated with a modified version of the LGPL'd work replacing the version originally provided to the user. When LGPL'd code is statically linked to a non-copyleft executable, for example, the required source code must also include sufficient material to split the distributed executable and relink with a modified version of the library.

Under §6(c), this source code may be offered in writing rather than provided, or it may be distributed by network under the terms of §6(d). In addition,

under §6(e) the distributor may "verify" that the user has already received, or at least that the distributor has already sent to this particular user, the relevant source. This is evidently intended to prevent requiring duplicate deliveries in "whole distribution" situations.

If the distributor of the combined work intends not to distribute or offer the source code of the LGPL'd components, the LGPL'd work must be separately distributed (subject to source code delivery requirements as part of that separate distribution) and packaged in a "shared library" mechanism, which means

> that [it] (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

Taken together, these provisions mean:

1. If you create a program that links through a shared library mechanism to a work that is separately distributed under LGPLv2.1, then you can distribute the resultant program under a license of your choice and you need not convey the LGPL'd work's source code. If you distribute the library along with your program, or are the separate distributor of the work in another context or as another product, you must distribute its corresponding source under the terms of LGPLv2.1 or GPLv2+, at your option.

2. If you choose to statically link or otherwise combine your program with an LGPL'd work, you may choose your own license for the work provided the license terms limitations for user modification, reverse engineering and debugging are met, and given that the LGPL'd components are still governed by LGPL's terms. You must offer or provide complete and corresponding source code for the LGPL'd components. The source code material provided must be sufficient to regenerate the combined work with a user-modified version of the LGPL'd components.

Non-compliance with LGPLv2.1 is relatively widespread, probably because misimpressions about its terms easily dispelled by reading them are equally common. In our practice we represent some licensors who enforce their rights on behalf of their users. Public disputes are infrequent, because parties who

are asked to square their behavior with the language of the license have always chosen to do so when politely but firmly requested.

LGPLv3

LGPLv3 was designed to rectify the architectural plan of the GNU family of licenses, by making the copyleft license from which LGPLv3 is a combination exception GPLv3. LGPLv3 is therefore an additional permission in the form provided for in GPLv3 §7, above.

Section 0: Additional Definitions Section 0 defines the "Library" it covers as a work that presents one or more interfaces at which a "use" can be made by an "Application." Class inheritance is "deemed" a use of an interface. An "Application," which is other program code using one or more "Library" interfaces can be combined with the code on the other side of the interfaces it uses to form a "Combined Work."

Section 1: Exception to Section 3 of the GNU GPL Section 1 excepts away the interference with use of LGPLv3 code as part of "effective technological measures" of access limitation for other copyrighted works provided otherwise by GPLv3 §3.

Section 2 Conveying Modified Versions Section 2 continues to require, as LGPLv2.1 §2(d) required, that the Library not be modified to require keys, tokens, tables, or other global non-argument data unrelated to function. This is again stated as a "good faith effort" requirement, but failure to cure on notice is strong evidence of the absence of good faith. Use of GPLv3 terms by removal of the additional permission, as provided for by GPLv3 §7, is the alternate path to compliance.

Section 3: Object Code Incorporating Material from Library Header Files Section 3 disposes entirely of the area of ambiguity in the use of header files and other such forms of Library material covered by LGPLv2.1 §5 by stating a rule applicable at the user's discretion to all such uses within copyright scope: giving notice that the library is used in the program and providing copies of GPLv3 and LGPLv3 along with the work.

Section 4: Combined Works Section 4 is the combination permission at the heart of LGPLv3. It restates the license limitation provision of LGPLv2.1 §2 to clarify that the terms on the Combined Work may not prohibit user modification of the Library code, or the debugging of such modifications to the Library code by means of whatever reverse engineering is necessary.

Section 4(d)(0) contains the source provision requirement, for the Minimal Corresponding Source, which "means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version [of the Library]." The alternative to the provision of source code is distribution by way of the "shared library" mechanism under §4(d)(1), described with respect to LGPLv2.1 §6, above.

In addition, §4(e) requires the delivery of "installation information" required to install the modified version of the Library in "user products" under GPLv3 §6. Where Library Minimal Corresponding Source is not made available under §4(d)(1), §4(e) reaffirms that "installation information" must still be compliantly delivered under the terms of GPLv3 §6.

All other provisions of GPLv3 are in force as previously described, and are not excepted by the additional permission granted in LGPLv3.

Understanding Your Compliance Responsibilities

In the preceding sections, we have explained why developers of free software use the GNU family of copyleft licenses, and we have presented a detailed review of the provisions of these licenses in relation to the licensors' intentions and objectives. In the following sections, we review the compliance responsibilities of parties "downstream" from copylefted projects, and we offer some general advice about responding to source code provisioning inquiries from users and compliance complaints from copyright holders.

Who Has Compliance Obligations?

The fundamental focus of the licenses, as we have previously explained, is the preservation of users' rights to run programs for any purpose, to copy, modify and share without restriction. Compliance obligations are parsimoniously

imposed by the licenses, only to the extent that the drafters of the licenses and the licensors' using them consider to be minimally necessary to protect downstream users' rights. Copyleft is the central pillar of that system: the requirement to "share and share alike" all works based on the copylefted code freely offered from upstream. The licenses' ancillary provisions are intended to prevent the dilution or flouting of the "share alike" principle. The GNU licenses create a "commons" in traditional economic vocabulary; the restrictions imposed by the license are "governance" or "management" rules for the commons, like fisheries quotas, or groundwater preservation regulations in land use. Parties' obligations to the commons depend on their role in relation to its resources. We can delineate those roles and their respective responsibilities as follows:

1. Users of code under the licenses have no obligations, only rights. They are entitled to read, study, understand, run, modify, reuse, and transform all code so licensed, to the extent the particular license on the work, and any applicable exceptions from its restrictions, dictate. In the exercise of these rights, they are entitled to possess and make use of the complete and corresponding source code of the work, which means each computer program in the form in which it is most convenient to be modified, along with the ancillary scripts, makefiles, etc. required to build modified versions of the program and any applicable installation information. Because such rights are useless unless users know of them, they must also receive actual notice of the terms covering the program.

2. Providers of services over networks—when they are using computer programs specifically designed to provide such services over networks and licensed under GNU AGPL—have the obligations described above to the users of those services.

3. Distributors of licensed works—whether they are distributing modified or unmodified versions of the works, whether they have embedded executable copies of licensed works in a device, or are selling or otherwise transferring only a digital copy—have obligations to at least the users to whom they or intermediary parties distributed those copies. Whether those obligations run also to third parties not directly receiving their distribution of the works depends on the precise license involved, and their chosen mode of either distributing or offering to distribute source code. In addition, they have obligations to upstream

parties, to preserve reasonable legal notices embedded in the code, and to mark modified versions appropriately.

4. Both service providers and distributors have the obligation, in order to protect users' rights, to refrain from imposing any additional restrictions on downstream parties. They must refrain from terms in "umbrella licenses," EULAs, or sublicenses that restrict downstream users' rights as described above. Under the terms of LGPL, they must also refrain from license terms on works based on the licensed work that prohibit replacement of the licensed components of the larger non-LGPL'd work, or prohibit decompilation or reverse engineering in order to enhance or fix bugs in the LGPL'd components.

5. Patent holders having claims reading on works they distribute have an obligation to refrain from enforcing those claims against parties to whom they distribute. Patent holders modifying and distributing works under the version 3 family of licenses have an obligation to refrain from enforcing any claims reading on the version they distributed, not only against that version as distributed, but also against any subsequent version or work based thereon that also practices those claims.

6. All parties have an obligation to refrain from acting as a provider of services or distributor of licensed works if they have accepted, or had imposed on them by judicial action, binding legal conditions that would prevent them from meeting obligations to users as described. If a party is under such conflicting obligations, it has a duty to refrain from playing the role in which it is no longer free to meet its license obligations.

How to Meet Compliance Obligations

In our experience of working with commercial parties building GPL compliance programs—as well as in our role as lawyers representing GPL licensors coping with the consequences of compliance failures—we have observed that there is a significant mismatch between the assumptions businesses make about compliance and the realities of what goes wrong, what causes disputes, and how those disputes are resolved. Often, we have found companies preparing at great expense to avoid unlikely risks that have low historical incidence of occurrence and low cost of remediation, while leaving unman-

aged the risks that have historically resulted in all the litigation and other adverse outcomes. In this section, we describe in broad terms the activities that help businesses prepare to meet their compliance obligations with minimal effort at minimal cost, dealing preventively with the compliance risks they really face.

The mismatch between actual compliance risk and compliance risk management, in our experience, results from a misunderstanding of licensor intentions. Commercial parties often expect copyleft project communities to approach compliance as a form of copyright monetization, or else as an ideological effort to force proprietary software to be relicensed under copyleft terms. Under the assumption that the intention of the licensors is to take advantage of non-compliance to extract royalties, or to force the business's proprietary products to be distributed under copyleft, businesses manage the risk that they will "accidentally"—or as the result of unsupervised activity by individual programmers—copy infringing "snippets" of copylefted code into their own proprietary computer program. Risk management involves the purchase of expensive proprietary "code scanning" services that purport to detect such accidental inclusions. Effort is concentrated on how proprietary computer programs are made, to prevent "infection" by free software.

In fact, however, development communities that use copyleft regard compliance failures as an opportunity to improve compliance. Every compliance failure downstream from their project represents a loss of rights by their users. The project, as copyright holder, is the guardian of its users' rights. Their activity is designed to restore those rights, and to protect the project's contributors' intentions in the making of their software. Projects' goals in seeking compliance are more often frustrated by the way software is delivered to users than by the way combinations of proprietary and free software are made. In particular,

- Users aren't provided with required information about the presence of copylefted programs and their applicable license terms in the product they have purchased; or
- Users can't reliably get complete and corresponding source code to copylefted programs the distributor knew it was using and intended to use pursuant to the license terms; or
- Users get no response when they communicate with published addresses requesting fulfillment of businesses' obligations.

In these and similar situations, the project's goal is compliance with obligations intentionally incurred by intentional use of copylefted programs, through observance of fulfillment obligations to downstream users. Failures of this type, which are uncaught by scanning programs or other similar services, have resulted in all the litigation ever brought by copyleft communities around the world.

Inclusions of free software in commercial proprietary products do happen. In our practice on behalf of copyleft-using development communities, we encounter such problems not frequently, but regularly. To the best of our knowledge, not one such instance has ever resulted in compliance litigation by a community party. These issues are regularly settled in an amicable and cooperative fashion.

The Key to Compliance is Governance

"Software governance" is the phrase we use to describe the processes by which businesses document and control what software they take in, what software they distribute, and what license terms they incur or offer on those inbound and outbound transactions. Whether the business is selling physical products with software embedded, or software products and services, good software governance is the key to minimum-cost preparation to meet compliance obligations.

Let's take a hypothetical manufacturer of consumer electronic devices, the Acme Company. Acme embeds Android—containing a copylefted OS kernel, Linux, and some custom applications containing LGPL'd libraries, along with some GPL'd utilities—in some devices. It embeds custom software stacks—also containing a copylefted kernel, modified Linux, Busybox under GPLv2, and a suite of GNU utilities under GPLv3—in others. It provides firmware upgrades, as digital files, to intermediaries who resell some of their devices. Acme chooses not to provide CDs or USB memory sticks containing GPL'd source code along with its products, preferring instead to place a written offer for relevant source code in product packaging or documentation. As a result, Acme has obligations to provide complete and corresponding source code for all copylefted programs in its products to any requesting party.

In order to meet these obligations, Acme's governance process begins from the "bill of materials" listing the component parts of the software stack in

each product it makes. "License analysis," a process for which good FOSS tools exist, is used to confirm the licenses applicable to all the items on the bill of materials before development begins, and in an iterated process as development continues and the bill of materials is modified. A set of license texts required to be reproduced in product documentation is built from the output of the license analysis step, and is included in the product packaging and online documentation. For any copylefted software Acme takes in—whether embedded in hardware components or provided by third-party software suppliers—it automatically requests complete and corresponding source code. By exercising its own rights as a user, Acme prepares to meet its own obligations, and improves the compliance responsiveness of entities in its supply chain.

All source code taken in by Acme under copyleft licenses is carried, modified or unmodified, through the build process. At every stage, from the first trial build to the final build for release to manufacturing, the complete and corresponding source code for the copylefted binaries is itself part of the build target. When the product containing this software stack is released, the complete and corresponding source for all copylefted components is placed on a public-facing website, indexed by the product model number, a revision code, or an arbitrary hash code specific to the device and software version. This "stackmark" is also printed in the product documentation, and is represented by a QR-code on the exterior product packaging. A similar stack mark accompanies firmware upgrades delivered as digital files to sales intermediaries for placement on their own websites.

Legal review before product release verifies that Acme's forbearance obligations are also met. Any EULA, or umbrella license Acme wraps around all the software in its products, and any services agreement it makes for "software as a service" deployments in connection with its products, is checked to assure that it explicitly defers to the terms of any FOSS licenses in the product software stack, thus assuring that no additional restrictions are imposed in violation of copyleft.

As a result of these steps in its software governance process, Acme is confident that any user of its products who wishes to exercise her or his rights under the GNU family of licenses can request and receive source code instantly, even without opening the box. Acme also can be sure that each purchaser of its products has been provided a copy of the relevant copyleft licenses, and that no licensing of its own proprietary products interferes with

or vitiates rights users have concerning copylefted software in their products, with minimum friction and at minimum cost.

These steps do not guarantee that Acme has avoided any accidental inclusion of copylefted code in a proprietary program it distributes as part of the product stack. But Acme has assured itself against the forms of compliance failure that have caused 100% of all the compliance litigation ever brought by community parties.

Principles of Prepared Compliance

Of course, the real world is not as simple as our schematic description of the Acme Company. Contemporary products, from cars to home appliances to networking or entertainment devices, may each contain dozens of computers, each containing in turn a full stack of embedded software, mixing copyleft FOSS, other FOSS, and proprietary programs. But a few basic principles remain valid across the entire complex domain:

1. Measure your compliance from the position of the user downstream from you trying to exercise rights conveyed by the licenses. Has the user received notice of the copylefted software intentionally included in your product? Is complete, corresponding source code and applicable installation information available to the user easily, preferably by automated means? Tools that measure what you deliver are more valuable than tools that only measure what you build.

2. Always exercise your own right to request complete and corresponding source code for all copylefted works from all your providers of software and of components embedding software, preferably in an automated process directly feeding your overall software governance system. Where possible, reject as non-conforming components provided to you containing copylefted software for which complete and corresponding source code is not furnished in response to your request or which is not accompanied by a "stackmark" for automated provisioning of source code. If you rely on an upstream provider for your software you cannot ignore your GPL compliance requirements simply because someone else packaged the software that you distribute.

3. Concentrate on the copylefted software you know you are using. Historically, the risk from a copylefted code snippet that some programmer dropped in your proprietary product careless of the consequences

is a problem far more infrequent and less difficult to resolve. Efficient management of the risks of higher concern lies in making sure you can provide, for example, precisely corresponding source code and makefiles for a copy of the Coreboot bootloader, Linux kernel, Busybox, or GNU tar that you included in a product you shipped two years ago.

4. Don't rely blindly on code scanners as they work too late in the process to improve your governance and too early in the process to catch problems in your delivery and post-sale provisioning. They do less important parts of the job expensively, and more important parts of the job not at all. Use them, where they are cost-effective, as a supplement to your own governance and verification processes, not as a primary tool of risk management.

Handling Compliance Inquiries

Between us, the authors have spent almost thirty person-years enforcing the GPL. We have, individually or collectively through SFLC, participated in every community enforcement of the GNU copyleft licenses ever brought to court in the United States. We have helped to settle dozens of compliance disputes for every one that has ever reached the point of litigation.

In this context, too, we have seen the consequences of mutual misunderstanding. Community parties bring forward complaints of non-compliance in order to achieve compliance. Commercial parties often expect compliance disputes to result in monetary demands or efforts to interfere with trade secret treatment of proprietary software, and respond defensively in consequence. Community parties, accustomed to the software engineering practices of the FOSS world, sometimes assume that commercial parties who cannot swiftly produce complete and corresponding source code for copylefted programs they intentionally included in their products are engaged in deliberate obfuscation.

In our experience, skilled facilitation of communication between parties at the early stages of the process can prevent these misunderstandings from escalating. A few guidelines about what to expect, accompanied by some historical examples, may help:

1. *Return the call with the right person.* The single most important rule of successful handling of compliance complaints is to maintain commu-

nication. Routing FOSS compliance issues to a particular individual who understands the internal software governance mechanisms, and can serve as the key public contact with the community when compliance concerns arise, may be the most effective way to resolve compliance matters. No community party has ever brought a compliance enforcement lawsuit against a party who responded cooperatively to its initial communications.

In one instance, a major multinational consumer electronics manufacturer which had repeatedly failed to respond to requests for fulfillment of source code obligations over many months was removed from a multi-defendant compliance enforcement lawsuit hours before the complaint was filed, as a result of mere verbal assurances of swift cooperation made personally by the corporation's general counsel in a telephone conversation with one of the present authors, who was acting on behalf of the complaining copyright holder.

2. *Assume preparation on the complainant's side.* The organizations traditionally bringing complaints of copyleft non-compliance (in historical order, the Free Software Foundation, GPL-violations.org, the Software Freedom Law Center, and the Software Freedom Conservancy) all fully investigate and verify complaints referred to them before making contact with apparently non-complying parties. Complainants will be prepared to substantiate the facts on which their complaint is based.

   In an unintended inclusion case arising some years ago, a global manufacturer used an entire copylefted library to provide essential features in one of its flagship proprietary software products. When we contacted them on behalf of the copyright holder, the corporation's legal counsel for FOSS matters repeatedly denied that such an event could have occurred, or that the code which our engineers could clearly see in their product was present there. We had to insist, three times, on their rechecking with their own engineers before they agreed that, indeed, such a mistake had occurred. Once our view of the facts had been verified, the matter was swiftly settled, without litigation and without payment of monetary damages.

3. *Let engineers be a part of the process.* The most time-consuming and difficult part of resolving most compliance matters, in our experience, is verifying that source code is indeed complete and corresponding. Without direct contact between software engineers on both sides, the resolution of the technical issues involved in demonstrating that the

binary distributed was built from the source provided is likely to be tortuous, expensive, and potentially tense. Counsel are understandably reluctant to expose their client's employees to direct inquiry from potentially hostile parties. But facilitated exchanges of information among software engineers communicating on technical subjects shortens the time to resolution, substantially reduces the cost of reaching resolution, and prevents unnecessary escalation due to mutual misunderstanding.

4. *Offer compliance.* Under the GPLv3 family of licenses, license termination is automatically reversed by prompt action to cure non-compliance, except in cases of repeated infringement. Although license termination is automatic under the terms of GPLv2, most of the GPLv2 licensors whose programs are widely used in commerce have a policy of immediately restoring distribution rights for non-compliant parties who come promptly into compliance when notified. An offer of compliance, subject to verification and mutual agreement on the details, is likely under all but the most exceptional circumstances to form the basis of an amicable settlement.

   In cases of mistaken inclusion of copylefted code in proprietary programs distributed as software products, prompt offer to remove the copylefted code and to redistribute a compliant version to customers and other reasonably reachable recipients has historically been the linchpin of arrangements to avoid litigation by amicable settlement.

5. *Use compliance discussions to improve relationships.* Development communities make software to benefit users, which includes you. When you use copylefted community software in your products, you are an important and valuable part of the commons, from the developers' point of view. Resolving a compliance matter is an occasion to strengthen your relationship to the commons, by increasing communication between your engineers and the project whose output you use for business benefit.

   In our experience, companies have often formed beneficial consulting or employment relationships with project developers they first encountered through compliance inquiries. In some cases, working together to alter the mode of use of the project's code in the company's products was an explicit element in dispute resolution. More often, the communication channels opened in the course of the inquiry served other and more fruitful purposes later.

6. *When the dust settles, offer to cover costs.* Most of the work investigating compliance complaints and verifying remediation is performed by non-profit entities that represent development communities without revenue. The ethic of these community parties against rent-seeking and monetization of others' mistakes means that the substantial engineering efforts they put into preparing compliance inquiries and resolving disputes are often paid for from their own scant means.[9] When a compliance issue has been successfully resolved, an offer to cover the cost of the engineering time involved on the community's side will do much to ensure the continuance of good relations in future. Requests for the repayment of those costs are entirely reasonable and foreseeable; a prompt offer precludes the escalation of dispute, an outcome we have seen more than once in our practice.

[9]SFLC provides free legal assistance to non-profit parties who make and distribute FOSS. Our efforts, including our work on compliance matters, are funded not from proceeds of settlement, but from the donations of companies and individuals who recognize the value of those services. SFLC has occasionally participated in monetary settlements made with non-compliant parties on behalf of projects we represent. Such settlements represent less than 2% of SFLC's historical revenues, and have never amounted to as much as 10% of our income in any fiscal year. We have not recouped in any settlement the cost of our efforts in that particular case, let alone the cost of our efforts on behalf of our clients overall.

Appendix 1: Offer of Source Code

From *A Practical Guide to GPL Compliance*[10]

Many distributors prefer to ship only an offer for source with the binary distribution, rather than the complete source package. This option has value when the cost of source distribution is a true per-unit cost. For example, this option might be a good choice for embedded products with permanent storage too small to fit the source, and which are not otherwise shipped with a CD but *are* shipped with a manual or other printed material.

However, this option increases the duration of your obligations dramatically. An offer for source must be good for three full years from your last binary distribution (under GPLv2), or your last binary or spare part distribution (under GPLv3). Your source code request and provisioning system must be designed to last much longer than your product life cycle.

In addition, if you are required to comply with the terms of GPLv2, you **cannot** use a network service to provide the source code. For GPLv2, the source code offer is fulfilled only with physical media. This usually means that you must continue to produce an up-to-date "source code CD" for years after the product's end-of-life.

Under GPLv2, it is acceptable and advisable for your offer for source code to include an Internet link for downloadable source *in addition* to offering source on a physical medium. This practice enables those with fast network connections to get the source more quickly, and typically decreases the number of physical media fulfillment requests. (GPLv3 §6(b) permits provision of source with a public network-accessible distribution only and no physical media. We discuss this in detail at the end of this section.)

The following is a suggested compliant offer for source under GPLv2 (and is also acceptable for GPLv3) that you would include in your printed materials accompanying each binary distribution:

> The software included in this product contains copyrighted software that is licensed under the GPL. A copy of that license is included in this document on page X. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of this product, which will be no earlier than 2011-08-01, by sending a money order or check for

[10] `http://softwarefreedom.org/resources/2008/compliance-guide.html`.

> $5 to:
> GPL Compliance Division
> Our Company
> Any Town, US 99999
>
> Please write "source for product *Y*" in the memo line of your payment.
>
> You may also find a copy of the source at
> `http://www.example.com/sources/Y/`.
>
> This offer is valid to anyone in receipt of this information.

There are a few important details about this offer. First, it requires a copying fee. GPLv2 permits "a charge no more than your cost of physically performing source distribution". This fee must be reasonable. If your cost of copying and mailing a CD is more than around $10, you should perhaps find a cheaper CD stock and shipment method. It is simply not in your interest to try to overcharge the community. Abuse of this provision in order to make a for-profit enterprise of source code provision will likely trigger enforcement action.

Second, note that the last line makes the offer valid to anyone who requests the source. This is because v2 §3(b) requires that offers be "to give any third party" a copy of the Corresponding Source. GPLv3 has a similar requirement, stating that an offer must be valid for "anyone who possesses the object code". These requirements indicated in v2 §3(c) and v3 §6(c) are so that non-commercial redistributors may pass these offers along with their distributions. Therefore, the offers must be valid not only to your customers, but also to anyone who received a copy of the binaries from them. Many distributors overlook this requirement and assume that they are only required to fulfill a request from their direct customers.

The option to provide an offer for source rather than direct source distribution is a special benefit to companies equipped to handle a fulfillment process. GPLv2 §3(c) and GPLv3 §6(c) avoid burdening noncommercial, occasional redistributors with fulfillment request obligations by allowing them to pass along the offer for source as they received it.

Note that commercial redistributors cannot avail themselves of the option (c) exception, and so while your offer for source must be good to anyone who receives the offer (under v2) or the object code (under v3), it *cannot* extinguish the obligations of anyone who commercially redistributes your

product. The license terms apply to anyone who distributes GPL'd software, regardless of whether they are the original distributor. Take the example of Vendor V, who develops a software platform from GPL'd sources for use in embedded devices. Manufacturer M contracts with V to install the software as firmware in M's device. V provides the software to M, along with a compliant offer for source. In this situation, M cannot simply pass V's offer for source along to its customers. M also distributes the GPL'd software commercially, so M too must comply with the GPL and provide source (or M's *own* offer for source) to M's customers.

This situation illustrates that the offer for source is often a poor choice for products that your customers will likely redistribute. If you include the source itself with the products, then your distribution to your customers is compliant, and their (unmodified) distribution to their customers is likewise compliant, because both include source. If you include only an offer for source, your distribution is compliant but your customer's distribution does not "inherit" that compliance, because they have not made their own offer to accompany their distribution.

The terms related to the offer for source are quite different if you distribute under GPLv3. Under v3, you may make source available only over a network server, as long as it is available to the general public and remains active for three years from the last distribution of your product or related spare part. Accordingly, you may satisfy your fulfillment obligations via Internet-only distribution. This makes the "offer for source" option less troublesome for v3-only distributions, easing compliance for commercial redistributors. However, before you switch to a purely Internet-based fulfillment process, you must first confirm that you can actually distribute *all* of the software under GPLv3. Some programs are indeed licensed under "GPLv2, *or any later version*" (often abbreviated "GPLv2-or-later"). Such licensing gives you the option to redistribute under GPLv3. However, a few popular programs are only licensed under GPLv2 and not "or any later version" ("GPLv2-only"). You cannot provide only Internet-based source request fulfillment for the latter programs.

If you determine that all GPL'd works in your whole product allow upgrade to GPLv3 (or were already GPLv3'd to start), your offer for source may be as simple as this:

> The software included in this product contains copyrighted software that is licensed under the GPLv3. A copy of that license is included in this document on page X. You may obtain the com-

> plete Corresponding Source code from us for a period of three years after our last shipment of this product and/or spare parts therefor, which will be no earlier than 2011-08-01, on our website at `http://www.example.com/sources/productnum/`.

Under both GPLv2 and GPLv3, source offers must be accompanied by a copy of the license itself, either electronically or in print, with every distribution.

References

1. Free Software Foundation, FSF FAQs about the GNU Licenses. http://www.gnu.org/licenses/gpl-faq.html, October 2014. (Accessed Oct 23, 2014).
2. Free Software Foundation, How to use GNU licenses for your own software. http://www.gnu.org/licenses/gpl-howto.html, April 2014. (Accessed Oct 23, 2014).
3. Free Software Foundation, Various Licenses and Comments about Them. http://www.gnu.org/licenses/license-list.html, October 2014. (Accessed Oct 23, 2014).
4. Bradley M. Kuhn, Aaron Williamson, Karen M. Sandler, A Practical Guide to GPL Compliance. http://softwarefreedom.org/resources/2008/compliance-guide.html, August 2008. (Accessed Oct 23, 2014).
5. Software Freedom Law Center, Managing Copyright Information Within a Free Software Project. http://softwarefreedom.org/resources/2012/ManagingCopyrightInformation.html, September 2012. (Accessed Oct 23, 2014).
6. A History of the GPLv3 Revision Process, Eben Moglen. https://www.softwarefreedom.org/resources/2013/A_History_of_the_GPLv3_Revision_Process.pdf, July 2013. (Accessed Oct 23, 2014).
7. Free Software Foundation, GPLv3 Discussion Draft 1. http://gplv3.fsf.org/comments/gplv3-draft-1, January 2006. (Accessed Oct 23, 2014).
8. Free Software Foundation, GPLv3 Discussion Draft 2. http://gplv3.fsf.org/comments/gplv3-draft-2, July 2006. (Accessed Oct 23, 2014).
9. Free Software Foundation, GPLv3 Discussion Draft 3. http://gplv3.fsf.org/comments/gplv3-draft-3, March 2007. (Accessed Oct 23, 2014).
10. Free Software Foundation, GPLv3 Discussion Draft 4. http://gplv3.fsf.org/comments/gplv3-draft-4, May 2007. (Accessed Oct 23, 2014).

The Principles of Community-Oriented GPL Enforcement

by Joshua Gay — Published on Sep 30, 2015 04:51 PM

The GNU General Public License (GPL) is the principal copyleft license. Copyleft is a framework that permits ongoing sharing of a published work, with clear permissions that *both* grant *and* defend its users' freedoms — in contrast to other free licenses that grant freedom but don't defend it. Free software released under the GPL is fundamental to modern technology, powering everything from laptops and desktops to household appliances, cars, and mobile phones, to the foundations of the Internet. Following the GPL's terms is easy — it gets more complicated only when products distributed with GPL'd software also include software distributed under terms that restrict users. Even in these situations, many companies comply properly, but some companies also try to bend or even break the GPL's rules to their perceived advantage.

The Free Software Foundation (FSF) and Software Freedom Conservancy (Conservancy) today lead worldwide efforts to ensure compliance with the GPL family of licenses. The FSF began copyleft enforcement in the 1980s, and Conservancy has enforced the GPL for many of its member projects since its founding nearly a decade ago. Last year, the FSF and Conservancy jointly published *Copyleft and the GNU General Public License: A Comprehensive Tutorial and Guide*, which includes sections such as "A Practical Guide to GPL Compliance" and "Case Studies in GPL Enforcement", which explain the typical process that both the FSF and Conservancy follow in their GPL enforcement actions. (Shorter descriptions of these processes appear in blog posts written by the FSF and Conservancy.)

As stalwarts of the community's freedom, we act as a proxy for users when companies impede the rights to copy, share, modify, and/or redistribute copylefted software. We require all redistributors to follow the GPL's requirements in order to protect all the users' freedom, and secondarily to support businesses that respect freedom while discouraging and penalizing bad actors.

Copyleft is based on copyright; it uses the power of copyright to defend users' freedom to modify and redistribute rather than to hinder modification and redistribution. A traditional copyright license is violated by giving the work to others without permission; a copyleft license is violated by imposing restrictions to *prevent* further redistribution by others. Nevertheless, with their basis in copyright law, copyleft licenses are enforced through the same mechanisms — using the same vocabulary and

processes — as other copyright licenses. We must take care, in copyleft enforcement, to focus on the ultimate freedom-spreading purpose of copyleft, and not fall into an overzealous or punitive approach, or into legitimizing inherently unjust aspects of the copyright regime. Therefore Conservancy and the FSF do enforcement according to community-oriented principles originally formulated by the FSF in 2001.

Guiding Principles in Community-Oriented GPL Enforcement

- **Our primary goal in GPL enforcement is to bring about GPL compliance.** Copyleft's overarching policy goal is to make respect of users' freedoms the norm. The FSF designed the GNU GPL's text towards this end. Copyleft enforcement done in this spirit focuses on stopping incorrect distribution, encouraging corrected distribution, and addressing damage done to the community and users by the past violation. Addressing past damage often includes steps to notify those who have already received the software how they can also obtain its source code, and to explain the scope of their related rights. No other ancillary goals should supersede full compliance with the GPL and respect for users' freedoms to copy, share, modify and redistribute the software.
- **Legal action is a last resort. Compliance actions are primarily education and assistance processes to aid those who are not following the license.** Most GPL violations occur by mistake, without ill will. Copyleft enforcement should assist these distributors to become helpful participants in the free software projects on which they rely. Occasionally, violations are intentional or the result of severe negligence, and there is no duty to be empathetic in those cases. Even then, a lawsuit is a last resort; mutually agreed terms that fix (or at least cease) further distribution and address damage already done are much better than a battle in court.
- **Confidentiality can increase receptiveness and responsiveness.** Supporters of software freedom rightly view confidentiality agreements with distrust, and prefer public discussions. However, in compliance work, initiating and continuing discussions in private demonstrates good faith, provides an opportunity to teach compliance without fear of public reprisal, and offers a chance to fix honest mistakes. Enforcement actions that begin with public accusations are much more likely to end in costly and lengthy lawsuits, and less likely to achieve the primary goal of coming into compliance. Accordingly, enforcers should, even if reluctantly, offer confidentiality as a term of settlement. If it becomes apparent that the company is misusing good faith confidentiality to cover inaction and unresponsiveness, the problems may be publicized, after ample warning.
- **Community-oriented enforcement must never prioritize financial gain.** Financial penalties are a legitimate tool to achieve compliance when used judiciously. Logically, if the only penalty for violation is simply compliance with the original rules, bad actors will just wait for an enforcement action before even reading the GPL. That social model for copyleft and its

enforcement is untenable and unsustainable. An enforcement system without a financial penalty favors bad actors over good ones, since the latter bear the minimal (but non-trivial) staffing cost of compliant distribution while the former avoid it. Copyright holders (or their designated agent) therefore are reasonable to request compensation for the cost of their time providing the compliance education that accompanies any constructive enforcement action. Nevertheless, pursuing damages to the full extent allowed by copyright law is usually unnecessary, and can in some cases work against the purpose of copyleft.

- **Community-oriented compliance work does not request nor accept payment to overlook problems.** Community-oriented enforcement cannot accept payments in exchange for ignoring a violation or accepting incomplete solutions to identified compliance problems. Ideally, copyright holders should refuse any payment entirely until the distributor repairs the past violation and commits formally (in writing) to plans for future compliance.
- **Community-oriented compliance work starts with carefully verifying violations and finishes only after a comprehensive analysis.** This means fully checking reports and confirming violations before accusing an entity of violating the GPL. Then, all of the relevant software should be examined to ensure any compliance problems, beyond those identified in initial reports and those relating to any clauses of the relevant licenses, are raised and fixed. This is important so that the dialogue ends with reasonable assurance for both sides that additional violations are not waiting to be discovered. (Good examples of compliance already exist to help distributors understand their obligations.)
- **Community-oriented compliance processes should extend the benefit of GPLv3-like termination, even for GPLv2-only works.** GPLv2 terminates all copyright permissions at the moment of violation, and that termination is permanent. GPLv3's termination provision allows first-time violators automatic restoration of distribution rights when they correct the violation promptly, and gives the violator a precise list of copyright holders whose forgiveness it needs. GPLv3's collaborative spirit regarding termination reflects a commitment to and hope for future cooperation and collaboration. It's a good idea to follow this approach in compliance situations stemming from honest mistakes, even when the violations are on works under GPLv2.

These principles are not intended as a strict set of rules. Achieving compliance requires an understanding of the violator's situation, not so as to excuse the violation, but so as to see how to bring that violator into compliance. Copyleft licenses do not state specific enforcement methodologies (other than license termination itself) in part because the real world situation of GPL violations varies; rigidity impedes success.

In particular, this list of principles purposely does not seek to create strict criteria and/or “escalation and mediation rules” for enforcement action. Efforts to do that limit the ability of copyright holders to use copyleft licenses for their intended effect: to stand up for the rights of users to copy, modify, and

redistribute free software.

The GPL, enforced when necessary according to these principles, provides a foundation for respectful, egalitarian, software-sharing communities.

This document is also published on Software Freedom Conservancy's site.

Copyright © 2015, Free Software Foundation, Inc., Software Freedom Conservancy, Inc., Bradley M. Kuhn, Allison Randal, Karen M. Sandler.

Licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.
The copyright holders ask that per §3(a)(1)(A)(i) and §3(a)(1)(A)(v) of that license, you ensure these two links ([1], [2]) are preserved in modified and/or redistributed versions.

[1]: https://sfconservancy.org/linux-compliance/principles.html

[2]: https://fsf.org/licensing/enforcement-principles

FOSS Compliance @ IBM
15 Years (and counting)

Terry Ilardi
Copyright Counsel-IBM

In the beginning…

- There was initial concern over use and distribution of FOSS licensed code
- *Each and every distribution* of FOSS code, whether written by the community or by IBM, was reviewed by an executive committee
  - with the assistance of an “expert team” (E-team) of attorneys and business people

What were the concerns?

- Provenance of the code
  - We had little familiarity with FOSS communities or how they worked
- Infringement of third party patents
- Loss of value of our own patent portfolio
- From the very start we took license compliance very seriously

Reviews Are a Joint Effort

- Local business and legal support work with developers to perform the initial reviews
- Developers answered a series of questions that established the contents, licenses and “trustworthiness” of the code

The Reviews

- Attorneys review the licenses
- Web searches
- Codescans using a home grown scanning tool
  - Codescans were run by the developers; the reports were reviewed by attorneys
- If a review revealed issues, project inquiries were made

The Number of Proposals Kept Increasing

- Reviews were hierarchical
- Line attorneys would make an initial review, which was presented to increasingly senior levels of attorneys and business people
  - and then would be presented to the E-team
- As the number of proposals increased this system became unwieldy and was discouraging use of FOSS

We Reevaluated our Process

- Goal became *to facilitate*
- *License compliance* became key
- Proposals were sorted by their potential for "problems"
- Certain communities had their own reviews
  - these became "trusted" communities
- We eliminated many multiple reviews
- And fewer proposals were deemed necessary for approval by the E-team

We Streamlined for Efficiency

- We saw many licenses repeatedly; some carried fewer obligations than others
  - Lead to a list of “approved” licenses
- We also realized that certain FOSS packages were used repeatedly
  - We established a database of package information for reference in subsequent reviews
  - Some packages were deemed so benign that they could be used without any additional reviews

Proposals Up-Reviews Down

- Fewer reviews now come to the E-team
  - Many reviews are “self certifying”
    - The E-team provides review criteria
    - If the facts meet that criteria the developers may self-certify
  - Most other reviews can be handled with one level of review

Our Process Continues to Evolve

- Trained a team of attorney supervised law school interns to perform many reviews
  - They are very eager!
- We work hard to find ways to allow use
- Focus remains on license compliance
- But, we continuously revise our process

Community Trademark Policies

Software Freedom Law Center
October 30, 2015

1) Software Freedom Law Center: A Legal Issues Primer for Open Source and Free Software Projects, Chapter 5 – Common Trademark Issues

2) Apache Software Foundation: Apache Trademark Policy

3) Debian Project: Trademark Policy

4) XBMC Foundation / Kodi: Trademark Policy

Software Freedom
Law Center

1995 Broadway, 17th Floor
New York, NY 10023–5882
tel +1–212–580–0800
fax +1–212–580–0898
www.softwarefreedom.org

A Legal Issues Primer for Open Source and Free Software Projects

Richard Fontana
Bradley M. Kuhn
Eben Moglen
Matthew Norwood
Daniel B. Ravicher
Karen Sandler
James Vasile
Aaron Williamson

Version 1.5.2
4 June 2008

Copyright © 2006, 2007, 2008, Software Freedom Law Center, Inc. Verbatim copying and distribution of this entire document is permitted in any medium; this notice must be preserved on all copies.

Chapter 5

Common Trademark Issues

Like other products, FOSS applications develop reputations over time as users come to associate an application's name with a particular standard of quality or set of features. Trademark law can help protect this relationship of trust and reliance that a project develops with its users; it allows the project to maintain a certain amount of control over the use of its brand. This document is intended to explain how FOSS developers can make effective use of their trademarks. However, because we do not know the specifics of your project, this document provides general information and not legal advice. If your FOSS project has a specific need for legal advice, please contact the Software Freedom Law Center or seek other legal counsel.

5.1 Choosing a Mark

The purpose of a trademark is to identify the source of a product. FOSS projects often use their names or logos to indicate that a particular distribution, module, or upgrade is an official release of the project. In order to make such indications meaningful, trademark law enables a trademark's owner to prevent others from using the mark in ways likely to cause confusion among potential users of the software. Because the law only protects a mark insofar as it serves this identifying function, the most important quality of a good trademark is distinctiveness. A name, logo, or phrase that does not distinguish your program from other products with substantial similarities is unlikely to be afforded trademark protection. For this reason, generic marks consisting of common words that describe the project (e.g., a music player called "Music Player") are generally poor choices.

The "strongest" marks (those afforded the most protection under trademark law) are those which have no other associations, such as a made-up word or an abstract design. Such marks are the least likely to cause consumer confusion[1] because their only meaning is to identify the product. However, these marks might be undesirable from a marketing perspective, even though it is a strong mark from a legal perspective. Often a project will want its mark to say something about the product's purpose. A project need not avoid descriptive marks entirely, but should avoid marks that consist largely of words and images that are generic to the industry or are very similar to those already used to identify similar products.

If two entities are using the same mark on similar goods (such as two software applications), the law favors the one who used it first. Therefore, in stark contrast to patents (see Chapter 4), FOSS developers *should* perform a thorough search before choosing a mark; it behooves a FOSS project to be as certain as possible their chosen mark is not already in use. The best search is one performed by an experienced trademark specialist, largely because she knows where to look. However, resources are also available for those who wish to search on their own. The U.S. Patent and Trademark Office (USPTO) provides the Trademark Electronic Search System (TESS), which allows users to freely search the USPTO's database of registered trademarks. A search of registered trademarks is not enough, however, since U.S. law also provides *some* trademark protection in the absence of registration. Consequently, you should also perform a thorough web search to determine whether anyone is using that unregistered mark.

5.2 Registered v. Unregistered Marks

Though unregistered marks have some legal protections (called "common law" rights), they are limited to those geographical areas where consumers actually identify the trademark with its source. Traditionally, a mark's geographic reach is defined by criteria such as where the product is sold and where it can be found in brick and mortar stores. Such metrics apply poorly to products which are only (or primarily) distributed online, and consequently their geographic reach for the purposes of unregistered trademarks is generally uncertain.

You can minimize this uncertainty by registering your trademark with either a state or the federal government. Registration grants much stronger protections for your trademark if someone else uses the mark in connection with goods similar to the ones described in your registration application. Registration with a state government grants these protections within the state, while registration

[1] "Consumer confusion" is an important test regarding trademark similarity used by the USPTO.

with the federal government grants them throughout the nation.

The protections conferred through registration are not absolute. If someone establishes that they were using the mark before you, their rights to the use of their unregistered mark will still apply. A thorough search prior to registration can help you avoid this situation and any resulting territorial conflict.

For the vast majority of FOSS projects, especially those distributed on the web, federal registration is preferable and sufficient. Though federal registration fees are significantly higher — $275 per mark per goods classification for a federal mark versus an average of $50 for state registration — distribution is rarely or never limited to a particular state. In addition to broader applicability, federally registered trademarks can be enforced in federal courts, and provide a better position from which to register and enforce trademarks internationally.

5.3 The Federal Registration Process

The USPTO's trademark registration process is relatively simple. You do not need a lawyer, and the entire process can be done online (in fact, online registration is strongly preferred; the USPTO charges an additional $100 for paper filing).

Most of the registration requirements are straightforward — a jpeg image of the mark, the date you first used the mark, etc. In addition to this basic information, the application requires that you provide a "specimen" demonstrating your use of the mark in association with a product. For a software product, the specimen can be:

- A picture of the software's physical packaging bearing the mark, if the product has been distributed physically;
- A screenshot of a webpage displaying both the mark and a download link;
- An advertisement for the product; or
- Any other image which demonstrates "the overall context" of how you have used the mark in association with the product.

The specimen requirement only applies if you are currently using the mark. You may also register a trademark based on an intent to use the mark in commerce within six months of registration.

Next, you should make sure that your project fits within one of the descriptions in the USPTO's Acceptable Identification of Goods & Services manual. This

manual classifies goods first by a general international goods class, and then by a more specific identification within that class. There are 34 goods classes, but most FOSS projects will be concerned exclusively with class 9, which applies broadly to computing goods. While some projects will relate to other classes (e.g. games, or software intended for use in the medical industry), even for these projects it is generally sufficient to register only in class 9.

If upon searching the identification manual you are not able to find an identification that applies to your project, you must request that an applicable identification be added to the manual before you can register. You may find several applicable identifications within class 9, as many are quite broad. Make note of all of them so as to make your application as comprehensive as possible; though you must pay a registration fee for each class within which you register a mark, you may select several identifications within a class without paying an additional fee.

After you have all of the above information, you should be able to complete the application without any problem. In order to file the (less expensive) online application, you must pay when you apply, either with a credit card or by setting up a deposit account with the USPTO prior to filing.

5.4 Using Your Mark

If a mark is no longer useful to distinguish one source of goods from another, it can lose its trademark protection, regardless of registration. This can happen either through abandonment or genericide. Abandonment occurs if the trademark holder stops using the mark for an extended period of time (usually over three years), or fails to monitor or control how the mark is used. Genericide generally occurs when the trademark comes to be used by consumers to refer to a general class of goods, rather than to the trademark holder's particular product, and the trademark holder does not take sufficient action to prevent such generic use of the mark. By observing the following "best practices" guidelines when using or licensing their marks, most projects should be able to easily avoid abandonment and genericide concerns.

5.4.1 Proper Use of Your Own Mark

When you use your trademark (e.g. on your website, packaging, documentation, advertising, and other materials), provide notice of your claim to the mark. If you have not registered your mark, you may use the "™" symbol to assert your common law rights. If your mark is registered, use the "®" symbol, "Registered,

U.S. Patent and Trademark Office," or "Reg. U.S. Pat. & Tm. Off."

Also, use your trademark in a consistent and distinctive manner. Set it apart from other text by using capitalized, italic, boldfaced, colored, or otherwise stylized text. Always use registered marks in the same form which appears in the registration application; do not pluralize singular marks.

Using a project's name in place of its function or general class increases the risk that the name will become generic and thus unprotected. A common example of this is "Aspirin"; formerly a trademark of Bayer, the name was used so frequently as a noun in place of "acetylsalicylic acid" that it became generic in the United States. Because software is functional by nature, there is a particular tendency for users to substitute a program's name for the function it performs (i.e., to use the mark as a verb, as in "grep"). You should avoid using your mark this way.

5.4.2 Others' Use of Your Mark

Trademark holders have the right to prevent the unauthorized use of their marks (or similar imitative designs) when such marks are used in commerce and are used in a manner that is likely to cause confusion or to deceive. Non-commercial use, such as in journalism or literature, is usually permissible. Even in connection with commercial goods and services, it is generally permissible for others to use your trademark in a manner that does not imply an official relationship or sponsorship (e.g., to indicate compatibility), to compare its software with yours, or to indicate that it sells or implements your software.

If you believe that someone is using your mark in a manner protected by your exclusive rights and has not obtained your authorization to do so, you should take action even if you do not object to their use. If you do not object, you should enter into an explicit license agreement with the other party, clearly defining the parameters of their use. It is particularly important to address in the license the quality of product to which your mark may be affixed. You may specify specific quality standards regarding testing, performance, compatibility, and the like. Alternatively, or additionally, you may explicitly retain the right to approve or veto individual uses of the mark. In practice, you should exercise your right to control use of the mark such that the reputation your users associate with your product is effectively upheld by your licensees.

If you disapprove of someone's unlicensed use which infringes upon your exclusive rights, you should send a polite email to the infringer notifying them of your claim to the mark, and that their use is unacceptable. You might suggest a licensing arrangement, contingent on some changes in their usage of the mark. If you believe such an arrangement is impossible, ask the violator to fix

the problem. Be polite but firm. It is often the case that license violations are inadvertent and easily fixed. Offer to help the violator take whatever steps are needed to achieve compliance, and avoid threats of publicity and lawsuits for as long as possible. Make sure the violator understands that your primary concern is the project's reputation, not a large financial settlement. Once you convince them of that point, they are likely to respond more positively even if they were initially unresponsive.

As described above, a trademark's legal protections can be lost if it becomes generic in the minds of the public. However, genericide occurs infrequently, and is a greater danger to very famous marks, simply because more widespread use gives rise to a greater possibility of widespread misuse. Furthermore, a trademark owner has no right to enjoin generic use where it is most common — in non-commercial communications amongst the public. Some trademark holders attempt to fight genericide by taking out advertisements clarifying proper use of their mark, but most FOSS projects do not have the finances for such a campaign. Instead, if you are concerned about genericide, you might post guidelines for proper use of your mark on your website. If you notice that someone is using the mark generically, you can point them to these guidelines and politely request that they help you protect your mark by using it properly. However, you have no legal right to stop non-commercial and non-confusing generic use, so demands and legal threats are particularly inappropriate in these communications.

5.5 An example: Project Foo and FooNews

A typical situation for a successful project is that websites spring up to serve the needs of the project's community. This is usually a welcome development, but it does often raise trademark concerns. Here we look at FooNews, a new website devoted to the latest developments in the Project Foo community. Such a website raises a few questions:

- Does the website need permission from the project to call itself "FooNews"?
- In what circumstances would a project want to stop such use of its trademark?
- How does a project give or deny permission to use their mark?

5.5.1 Is permission needed?

Most people, upon visiting a site called FooNews and seeing it report exclusively on news about Project Foo, would be quite likely to assume the site is owned

and controlled by Project Foo. It's a reasonable mistake as to the source of the website, and it is precisely this kind of mistake that trademark law aims to prevent. The way the law accomplishes this is to give the trademark holder the power to decide who may use the trademark and who may not. In virtually all cases of the kind described here, the trademark holder does indeed have the power to stop websites from using the mark for the purpose of preventing confusion as to the source of the website.

There are, however, other ways to prevent this confusion in the website's readers. The site could, for example, provide conspicuous disclaimers alerting readers to the fact that the site is operated by entirely different people than the project, that the views expressed and claims made by the site are not those of Project Foo or the people who work on Project Foo. If these disclaimers are conspicuous and definitive enough, that might remove the confusion and allow the site to use the trademark without the project's permission. Still, to avoid any doubts, it's best for both the project and the website to reach an agreement as to what use is permissible.

5.5.2 When to allow use

Way down in the roots of Software Freedom are the same ideas from which the belief in free speech derives. FOSS projects are not often built by people who value censorship, and there is a strong belief within most FOSS communities that projects should thrive on their merits, and not use legal weapons to silence critics and competitors. It is for this reason that in many cases, projects will encourage use of their name even when commercial, proprietary software-producers would forbid it.

The case of Project Foo and FooNews is no different. Although Project Foo can often stop a website like FooNews, it usually has no reason to do so. Calling the site "FooNews" is an excellent way to communicate to readers what the site is about, and Project Foo usually wants people to be able to find information about them. FOSS projects are built by nurturing community, not by using trademark law to crush it.

Sometimes, a project's community can be mean-spirited or critical of the project. Even then, if criticism is offered in good faith, a website like FooNews devoted to pointing out flaws in Project Foo might be useful. In any event, trademark enforcement against people who criticize a project will just engender more criticism. We encourage projects to encourage community-based websites related to the project, even when those websites contain criticism of the project.

The time to become concerned is when people want to use a trademark for purposes that don't further the project's goals. If people trade on your good

reputation to sell services that devalue or compete with your project (for example, by implying you endorse their products), it would be foolish *not* to do something about it.

Every project has different goals and every project's community is going to have a different idea of what is acceptable use of the project's name. Whatever action you decide to take with regard to the project's name, make sure your community understands the reasons why you make the decisions you do. If there is a lot of objection to your policies, you might want to examine them and see if there are ways to allow use while still protecting the project's name.

5.6 Trademark Policy

The default trademark rules are sufficient for most Software Freedom projects and most projects do not actually need a trademark policy. Sometimes, though, there is confusion in a project's community of developers and users as to what constitutes legal or acceptable use of the project's name or logo.

Most of the time, a project wants to encourage activity related to the project. When websites spring up that are devoted to supporting a project's users, providing related software and services, and discussing news about the project, that is a good sign that the project is successful and having a wide impact.

Here is a sample trademark policy that Project Foo could use to communicate some simple guidelines to its community about using their name and logo. You can adjust it to suit the needs of your project.

> We at Project Foo love it when people talk about Project Foo, build businesses around Project Foo and produce products that make life better for Project Foo users and developers. We do, however, have a trademark, which we are obliged to protect. The trademark gives us the exclusive right to use the term to promote websites, services, businesses and products. Although those rights are exclusively ours, we are happy to give people permission to use the term under most circumstances.
>
> The following is a general policy that tells you when you can refer to the Project Foo name and logo without need of any specific permission from Project Foo:
>
> First, you must make clear that you are not Project Foo and that you do not represent Project Foo. A simple disclaimer on your home page is an excellent way of doing that.

> Second, you may not incorporate the Project Foo name or logo into the name or logo of your website, product, business or service.
>
> Third, you may use the Project Foo name (but not the Project Foo logo) only in descriptions of your website, product, business or service to provide accurate information to the public about yourself.
>
> Fourth, you may not use the Project Foo graphical logo.
>
> If you would like to use the Project Foo name or logo for any other use, please contact us and we'll discuss a way to make that happen. We don't have strong objections to people using the name for their websites and businesses, but we do need the chance to review such use. Generally, we approve your use if you agree to a few things, mainly: (1) our rights to the Project Foo trademark are valid and superior to yours and (2) you'll take appropriate steps to make sure people don't confuse your website for ours. In other words, it's not a big deal, and a short conversation (usually done via email) should clear everything up in short order.
>
> If you currently have a website that is using the Project Foo name and you have not gotten permission from us, don't panic. Let us know, and we'll work it out, as described above.

5.7 Forking a Project

When a project forks, it may be desirable for the forked project to continue using the original project's marks in some form. In many situations, this is entirely consistent with the purpose of trademarks. If the fork is initiated by existing project members, it is appropriate for the fork to associate itself with the goodwill and reputation of those members who helped develop and promote the original project's marks. Often, common sense or convention supports such use; for example, a fork aimed at creating a mobile version of Project N might call itself "Project N Mobile." On the other hand, the original project may also have legitimate concerns that a fork's use of the mark will cause confusion or unwanted associations in the minds of users.

In order to balance the interests of the projects and minimize conflict, the leadership of the original and forking projects should, before the fork occurs, negotiate an agreement concerning the latter's use of the former's marks. The agreement might provide, for example, that the name of the original project may be incorporated within the fork's name, but may not be used independently to refer to the fork; or that the original project's graphical logo may only be used if it is sufficiently modified so that it clearly refers only to the fork.

Unfortunately, forking does not always occur under circumstances conducive to

amicable negotiation. In order to avoid negotiating terms amidst the ill will generated by a "bad breakup," we advise projects to decide on terms outlining acceptable use of trademarks by project forks before a fork is even contemplated, and to place these terms in a membership agreement or policy statement. A membership agreement, of course, would not apply to non-members who seek to fork the project.

5.8 Responding to Cease-And-Desist Letters

Cease-and-desist (or "demand") letters are often the first contact a company will make with someone it believes has infringed its trademark rights. They will typically describe the offending behavior and the applicable laws and penalties, and will demand some action on the part of the recipient (such as removing offending content from a website or product). Often these letters take a threatening tone that can be very intimidating, particularly to recipients who have neither the legal knowledge to evaluate the claims nor the resources to hire a lawyer.

When FOSS developers receive such cease-and-desist letters, it usually is because they have developed some software that replaces an existing proprietary product, and they have chosen a name that closely resembles the mark of that well-known proprietary application. To avoid the likelihood that this will happen to your project, follow the advice in § 5.1 to make your best effort to chose a name that does not resemble existing marks already in use.[2]

If you nevertheless receive a cease-and-desist letter, do not take for granted that its tone reflects the strength of the sender's legal position; the purpose of these letters is generally to inspire compliance with minimal effort, and sometimes scare tactics are effective to this end. Instead, respond reasonably. If the claims in the letter are unclear, ask for more information. Precisely what about your use is objectionable? What statute does the company believe you have violated? If after gathering this information, you are uncertain whether your use is infringing, contact the Software Freedom Law Center or seek other legal counsel.

Copyright © 2006, 2007, 2008, Software Freedom Law Center, Inc. Verbatim copying and distribution of this entire document is permitted in any medium; this notice must be preserved on all copies.

[2] It turns out that classic FOSS "hacker wordplay" names like "GNU" are actually an excellent way to avoid possible trademark infringement claims. Since "GNU" itself does not resemble the word "Unix" at all, and since when expanded it explicitly tells the reader that the product is **not** Unix (i.e., "Gnu's Not Unix"), a potential trademark holder on the term "Unix" would be hard pressed to make the case that consumers would be confused and think that GNU really is Unix.

Apache Trademark Policy

Available from: https://www.apache.org/foundation/marks/

This document outlines the policy and guidelines of the Apache Software Foundation (ASF) for the trademarks and graphic logos we use to identify Apache® projects and any software developed and distributed by Apache projects. The Apache Software Foundation owns all Apache-related trademarks, service marks, and graphic logos.

The following information helps ensure our marks and logos are used in approved ways, while making it easy for the community to understand the guidelines. If you have any questions about the use of logos or trademarks that are not addressed in these guidelines, please contact us.

Quick Links

- Rationale
- Who We Are
- Description of Key Trademark Principles
- Specific Guidelines
- Guidelines for Domain Names
- Guidelines for Events
- List of Apache Trademarks
- Frequently Asked Questions
- Apache Project Branding Guidelines (for PMCs)
- Process for ensuring suitable project and product names (for PMCs)

Rationale

Apache® trademarks, service marks, and graphics marks are symbols of the quality and community support that people have come to associate with projects of the Apache Software Foundation (ASF). To ensure that the use of Apache marks will not lead to confusion about our software, we must control their use in association with software and related services by other companies. Also, as a US based corporation, we have a legal responsibility and the authority to set guidelines for the use of our marks.

The Apache Software Foundation and its software must be clearly distinguishable from any software that competes with ASF software, and from software or services by any company or individual that is not part of Apache Software Foundation.

Our marks must not be used to disparage the Apache Software Foundation, our projects, members, sponsors, or communities, nor be used in any way to imply ownership, endorsement, or sponsorship of any ASF-related project or initiative of any kind.

Who We Are

The VP, Apache Brand Management and associated Brand Management Committee is the formal body within the ASF responsible for setting policy and answering questions about the use of our logos and trademarks, along with other responsibilities. The Committee is made up of elected members of the ASF who have shown merit in the branding and trademarks areas. The current VP, Apache Brand Management is Shane Curcuru, as appointed by the Board of Directors.

Description of Key Trademark Principles

This document is not intended to summarize the complex law of trademarks. It will be useful, however, to understand the following key principles:

What is a trademark?

A **trademark** is a word, phrase, symbol or design, or a combination of words, phrases, symbols or designs, that identifies and distinguishes the source of the goods of one party from those of others. A **service mark** is the same as a trademark, except that it identifies and distinguishes the source of a service rather than a product. Throughout this policy document, the terms "trademark" and "mark" refer to both trademarks and service marks.

These rules are generalized to describe ASF software associated with the trademark "Apache Foo", or more generally "Foo" when it is understood to refer to this specific Apache Foo software. Like most ASF software, this Foo software is maintained by the Apache Foo project, or by the Foo sub-project of another project, such as the "Apache Incubator" (itself an ASF trademark).

ASF's trademarks are either words (e.g., "Apache" and "Apache Foo" and "Foo") or graphic logos that are intended to serve as trademarks for that Apache software. The Apache feather is also an ASF

trademark for Apache software which has special meaning for ASF and special rules regarding its use.

Within the ASF, during our product release activity and on ASF websites, we will make sure that our trademarks are marked with a (TM) or (R) symbol or shown with trademark notices where appropriate so that everyone will recognize them as ASF trademarks, and by providing a list of ASF trademarks.

What is nominative use?

Anyone can use ASF trademarks if that use of the trademark is nominative. The "nominative use" (or "nominative fair use") defense to trademark infringement is a legal doctrine that authorizes everyone (even commercial companies) to use another person's trademark as long as three requirements are met:

1. The product or service in question must be one not readily identifiable without use of the trademark; (for example, it is not easy to identify Apache Hadoop software without using the trademark "Hadoop")
2. Only so much of the mark or marks may be used as is reasonably necessary to identify the product or service; and
3. The organization using the mark must do nothing that would, in conjunction with the mark, suggest sponsorship or endorsement by the trademark holder.

The trademark nominative fair use defense is intended to encourage people to refer to trademarked goods and services by using the trademark itself. This trademark defense has nothing to do with copyright fair use and should not be confused with those rules.

What is the "confusing similarity" or "likelihood of confusion" test?

Some uses of another person's trademark are nominative fair use, but some uses are simply infringing. Indeed, if a trademark is used in such a way that the relevant consuming public will likely be confused or mistaken about the source of a product or service sold or provided using the mark in question, then likelihood of confusion exists and the mark has been infringed.

Note that, even if there is no likelihood of confusion, you may still be liable for using another company's trademark if you are blurring or tarnishing their mark under the state and/or federal dilution laws.

To avoid infringing ASF's marks, you should verify that your use of our marks is nominative and that you are not likely to confuse software consumers that your software is the same as ASF's software or is endorsed by ASF. This policy is already summarized in section 6 of the Apache License , and so it is a condition for your use of Apache software:

> This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

Specific Guidelines

The following Specific Guidelines apply to the "Apache" word trademark and the "Apache feather" graphic trademark, as well as the trademarks and graphic logos for typical "Apache Foo" and "Foo" software produced by each of the ASF's projects. You may refer to our list of most Apache marks.

Examples of permitted nominative fair use:

- " *Free copies of Foo software under the Apache License and support services for Foo are available at my own company website.* "
- " *Derivative works of Foo software and support services for those derivative works are available under my own trademarks at my website.* " Please remember that, under trademark law, you may not apply trademarks to your derivative works of Foo software that are confusingly similar to "Foo" or "Apache Foo" or the Foo graphic logo trademarks.
- " *Foo software is faster (or slower) than Myco software.* "
- " *I recommend (or don't recommend) Foo software for your business.* "
- " *This <here> is the graphic logo for Apache Foo software.* "

Using Apache trademarks in book and article titles:

You may write about Apache Foo software, and use our trademarks in book or article titles. You needn't ask us for permission to refer to Foo, as in "Foo for Dummies", or "Explaining Foo", or "Foo Simplified", or "O'Reilly Guide to Foo", or even "Avoiding Foo".

We prefer that you refer to "Apache Foo" rather than simply "Foo" in the title if it fits, and we request that you clearly identify that "Apache", "Apache Foo", and "Foo" are trademarks of the Apache Software Foundation wherever you normally acknowledge important trademarks in your book or article.

For more details, please see our FAQ about Apache marks in publishing.

Using the Apache feather logo to identify ASF and link to www.apache.org :

The Apache feather logo is a special trademark to the members of the Apache Software Foundation and we intend to prevent its use in association with other companies' software or related services.

You needn't ask us for permission to use the Apache feather logo (the version published by us here) on your own website solely as a hyperlink to www.apache.org, or in other materials, such as presentations and slides, solely as a means to refer to the ASF itself.

All other uses of the Apache feather logo must be approved in writing by the VP, Apache Brand Management or by a member of the Brand Management Committee.

Using the Apache Foo or similar project graphic logos:

Graphic logos are contributed to ASF by artists as a way of creating a symbol with which the Apache project software can be identified. Examples of logos are the Hadoop elephant, the SpamAssassin arrow, or even the graphic way that the word "Maven" is spelled with an orange letter "a". Those graphic logos are special to the Apache projects that mark their software and their project websites with those logos.

You needn't ask us for permission to use Apache's graphics logos (the versions published on individual project's websites) on your own website solely as a hyperlink to the specific Apache project website or to www.apache.org. All other uses of Apache Foo (and similar) graphic logos must be approved in writing by VP, Apache Brand Management, member of the Brand Management Committee, or the relevant Apache projects' VP.

Unlike ASF's word trademarks (such as "Apache" and "Foo"), our graphic logos are also licensed to the public under the Apache License. That license permits you to create derivative works of those logos, as with any other Apache copyrighted work. However, trademark law does not allow you to apply any "confusingly similar" derivative logo to software if a relevant consumer would likely be confused by that use of that derivative logo.

If you have any questions or concerns about the use of or changes to any ASF graphic trademark, please contact us

Using Apache trademarks on merchandise:

You must obtain prior written approval from the VP, Apache Brand Management or designee to apply the "Apache", "Apache Foo" or "Foo" trademarks or their graphic logos to any merchandise that is intended to be associated in people's minds with Apache Foo software or any Apache software.

Permission to apply ASF trademarks (including graphic logos) may be granted for merchandise that promotes the Apache Software Foundation, the Apache Foo project and Foo software.

Permission to apply ASF trademarks will ordinarily be denied for merchandise that disparages Apache software or projects or that would serve to detract from the value of Apache software and its brands.

The following uses of ASF trademarks are probably infringing:

- Confusingly similar software product names.
- Software service offerings that are for anything other than official ASF-distributed software.
- Company names that may be associated in customer's minds with ASF or its trademarked project software.

Using Apache Trademarks in domain names

You may not use ASF trademarks such as "Apache" or "ApacheFoo" or "Foo" in your own domain names if that use would be likely to confuse a relevant consumer about the source of software or services provided through your website, without written approval of the VP, Apache Brand

Management or designee. You should apply the "likelihood of confusion" test described above, and please realize that the use of ASF trademarks in your domain names is generally not "nominative fair use."

For more details, please see our Domain Name Branding Policy.

Using Apache Trademarks in relation to conferences and events

Certain ASF trademarks are reserved exclusive for official Apache Software Foundation activities. For example, "ApacheCon" is our exclusive trademark for our regular ASF conferences, and the Apache feather is intended for ASF use at events in which we participate.

Individual ASF projects (such as "Apache Foo") often create their own conferences and events, or join with other organizations or companies to hold joint conferences or events. Any conflicting use of ASF trademarks (including trademarks related to our projects or products) in relation to conferences or events must be approved in writing from the VP, Apache Brand Management or designee.

For more details, please see our Event Branding Policy.

Important Note

Nothing in this ASF policy statement shall be interpreted to allow any third party to claim any association with the Apache Software Foundation or any of its projects or to imply any approval or support by ASF for any third party products or services.

Policy Version

This is version 1.1 of this Apache policy document, published in 2014.
Significant changes will be marked with a new version number.

v1.1 Update to have permissions by VP, Brand **or** designee

Copyright © 2015 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

Debian Trademarks: Trademark Policy

Version: 2.0
Published: 19 January 2013

Available from: https://www.debian.org/trademark#policy

Software in the Public Interest, Inc. owns a number of trademarks in both word and logo form including brands, slogans, styles. This policy encompasses all marks, in word and logo form, collectively referred to as Debian trademarks. You can see a non-exhaustive list of Debian trademarks, including both registered and unregistered (but otherwise legally recognized) trademarks at our trademarks page.

The objective of this trademark policy is:

1. to encourage widespread use and adoption of the Debian trademarks,
2. to clarify proper usage of Debian trademarks by third parties,
3. to prevent misuse of Debian trademarks that can confuse or mislead users with respect to Debian or its affiliates.

Please note that it is not the goal of this policy to limit commercial activity around Debian. We encourage businesses to work on Debian while being compliant with this policy.

Following are the guidelines for the proper use of Debian trademarks by publishers and other third parties. Any use of or reference to Debian trademarks that is inconsistent with these guidelines, or other unauthorized use of or reference to Debian trademarks, or use of marks that are confusingly similar to Debian trademarks, is prohibited and may violate Debian trademark rights.

Any use of Debian trademarks in a misleading and false manner or in a manner that disparages Debian, such as untruthful advertising, is always prohibited.

When You Can Use the Debian Trademarks Without Asking Permission

1. You can use Debian trademarks to make true factual statements about Debian or communicate compatibility with your product truthfully.
2. Your intended use qualifies as nominative fair use of the Debian trademarks, i.e., merely identifying that you are talking about Debian in a text, without suggesting sponsorship or endorsement.
3. You can use Debian trademarks to describe or advertise your services or products relating to Debian in a way that is not misleading.
4. You can use Debian trademarks to describe Debian in articles, titles or blog posts.
5. You can make t-shirts, desktop wallpapers, caps, or other merchandise with Debian trademarks

for *non-commercial usage*.

6. You can also make merchandise with Debian trademarks for *commercial usage*. In case of commercial usage, we recommend that you truthfully advertise to customers which part of the selling price, if any, will be donated to the Debian project. See our donations page for more information on how to donate to the Debian project.

When You Can NEVER Use the Debian Trademarks Without Asking Permission

1. You cannot use Debian trademarks in any way that suggests an affiliation with or endorsement by the Debian project or community, if the same is not true.
2. You cannot use Debian trademarks in a company or organization name or as the name of a product or service.
3. You cannot use a name that is confusingly similar to Debian trademarks.
4. You cannot use Debian trademarks in a domain name, with or without commercial intent.

How to Use the Debian Trademarks

1. Use the Debian trademarks in a manner that makes it clear that your project is related to the Debian project, but that it is not part of Debian, produced by the Debian project, or endorsed by the Debian project.
2. Acknowledge Software in the Public Interest, Inc.'s ownership of the Debian trademark prominently.

   Example:

   [TRADEMARK] is a (registered, if applicable) trademark owned by Software in the Public Interest, Inc.

3. Include a disclaimer of sponsorship, affiliation, or endorsement by Debian on your website and on all related printed materials.

   Example:

   X PROJECT is not affiliated with Debian. Debian is a registered trademark owned by Software in the Public Interest, Inc.

4. Distinguish the Debian trademarks from the surrounding words by italicizing, bolding or underlining it.
5. Use the Debian trademarks in their exact form, neither abbreviated or hyphenated, nor combined with any other word or words.
6. Do not create acronyms using the Debian trademarks.

Permission To Use

When in doubt about the use of Debian trademarks, or to request permission for uses not allowed by this policy, please send an email to trademark@debian.org with subject Trademark Use Request; be sure to include the following information in the body of your message:

- Name of the User
- Name of the organization/project
- Purpose of Use (commercial/non-commercial)
- Nature of Use

Newer Versions of this Policy

This policy may be revised from time to time and updated versions shall be available at https://www.debian.org/trademark.

Guidelines for Using Logos

- Any scaling must retain the original proportions of the logo.
- Do not use the Debian logos as part of your company logo or product logo or branding itself. They can be used as part of a page describing your products or services.
- You need not ask us for permission to use logos on your own website solely as a hyperlink to the Debian project website.

For any queries with respect to these guidelines, please send an email to trademark@debian.org.

Copyright © 1997-2014 SPI and others; See license terms
Debian is a registered trademark of Software in the Public Interest, Inc.

XBMC Foundation / Kodi Official:Trademark Policy

From Kodi

Available from: http://kodi.wiki/view/Official:Trademark_Policy

Contents

- 1 List of XBMC Foundation Trademarks
- 2 Introduction
- 3 Overall Guidelines for Printed Materials and Web Sites
- 4 Software Distributions
  - 4.1 Unaltered Binaries
  - 4.2 Modifications
  - 4.3 Add-ons, Skins and other extensions
  - 4.4 Related Software
- 5 Domain Names
- 6 Services Related to XBMC Foundation Software
- 7 XBMC Foundation Marks and Merchandise
- 8 Things You Can Do—Summary
- 9 Reporting Trademark Abuse
- 10 Questions

1 List of XBMC Foundation Trademarks

You can see a **complete list** of the XBMC Foundation trademarks. As other trademarks are created or registered, this list will be updated. As used in this policy, "trademarks" means not just the XBMC Foundation's logos, but also the names of its various products and projects, also called word marks, (collectively "XBMC Foundation Marks").

2 Introduction

This document outlines the policy of the XBMC Foundation regarding the use of the XBMC Foundation Marks. Any use of any XBMC Foundation trademark must be in accordance with this policy. Any use that does not comply with our trademark policy or does not have written authorization from us is not authorized. Any goodwill generated by the use of any XBMC Foundation Marks inures to the benefit of XBMC Foundation.

XBMC Foundation's Trademark Policy attempts to balance two competing interests: the XBMC Foundation's need to ensure that the XBMC Foundation Marks remain reliable indicators of quality,

source, and security; and XBMC Foundation's desire to permit community members, software distributors, and others with whom XBMC Foundation works to discuss XBMC Foundation's products and to accurately describe their affiliation with us. Striking a proper balance is a tricky situation that many organizations—in particular those whose products are distributed electronically—wrestle with every day and we've attempted to balance it here.

Underlying our trademark policy is the general law of trademarks. Trademarks exist to help consumers identify, and organizations publicize, the source of products. Some organizations make better products than others; over time, consumers begin to associate those organizations (and their trademarks) with quality. When such organizations permit others to place their trademarks on goods of lesser quality, they find that consumer trust evaporates quickly. That's the precise situation that the XBMC Foundation seeks to avoid. People's trust in our name and products is crucial to us—especially, when it comes to intangible products like software, trust is all consumers have to decide on which product to choose. We also are the caretakers of the trust our community members have placed in us. We created this Trademark Policy to protect both the public's and our community's trust in the XBMC Foundation Marks.

On an all too frequent basis, we receive reports about websites selling the XBMC Foundation's Kodi, using the XBMC Foundation Marks to promote other products and services, or using modified versions of the XBMC Foundation Marks. The problem with these activities is that they may be deceptive, harm users, cause consumer confusion, and jeopardize the identity and meaning of the XBMC Foundation Marks. Such cases range from good intentions but improper use of the trademarks (e.g., overenthusiastic fans), to people intentionally trading on the brand for their own benefit and/or to distribute modified versions of the product, to a clear intent to deceive, manipulate and steal from users in a highly organized and syndicated fashion. When we are notified of such activities, or identify problematic activities, we analyze the those situations and treat each case individually based on the intent and severity of the matter.

In creating our trademark policy, we seek to clarify the uses of the XBMC Foundation Marks we consider legitimate and the uses we do not. Although XBMC Foundation's Trademark Policy is composed of a number of specific rules, some contained in companion documents, most reflect the overarching requirement that your use of the XBMC Foundation Marks be non-confusing and non-disparaging. By non-confusing, we mean that people should always know whom they are dealing with, and where the software they are downloading comes from. Websites and software that are not created or produced by XBMC Foundation should not imply, either directly or by omission, that they are. By non-disparaging, we mean that, outside the bounds of fair use, you can't use the XBMC Foundation Marks as vehicles for defaming us or sullying our reputation. These basic requirements can serve as a guide as you work your way through the policy.

Our Trademark Policy begins by outlining some overall guidelines for the use of the XBMC Foundation Marks in printed materials. It then addresses a series of more specific topics, including the use of XBMC Foundation's trademarks on distributions of XBMC Foundation's binaries, linking to XBMC Foundation's website(s), and the use of XBMC Foundation Marks in domain names. At various

points, this policy links to other documents containing additional details about our policies.

We also have a **trademark policy FAQ** as a companion document to this policy.

3 Overall Guidelines for Printed Materials and Web Sites

We encourage the use of the XBMC Foundation Marks in marketing, and other publicity materials related to XBMC Foundation or the relevant XBMC Foundation product. This includes advertising stating that a person or organization is shipping XBMC Foundation products. Of course, any use of a XBMC Foundation trademark is subject to the overarching requirement that its use be non-confusing. Thus, you can't say you're raising money for XBMC Foundation when you're actually raising it for a localization project, say that you're reviewing or distributing the XBMC Foundation Kodi when you're actually reviewing or distributing a modified version of Kodi, or use the XBMC Foundation logos on the cover of your book or on your product packaging.

Although many uses of the XBMC Foundation Marks are governed by more specific rules, which appear below, the following basic guidelines apply to almost any use of the XBMC Foundation Marks in printed materials, including marketing, articles and other publicity-related materials, and websites:

- Proper Form - XBMC Foundation's trademarks should be used in their exact form -- neither abbreviated nor combined with any other word or words (e.g., "Kodi" rather than "KMC" or "KEC");
- Accompanying Symbol - The first or most prominent mention of a XBMC Foundation trademark should be accompanied by a symbol indicating whether the mark is a registered trademark ("®") or an unregistered trademark ("™"). See our **Trademark List** for the correct symbol to use;
- Notice - The following notice should appear somewhere nearby (at least on the same page or on the credits page) the first use of a XBMC Foundation trademark: "[TRADEMARK] is a ["registered", if applicable] trademark of the XBMC Foundation";
- Distinguishable - In at least the first reference, the trademark should be set apart from surrounding text, either by capitalizing it or by italicizing, bolding or underlining it. In addition, your website may not copy the look and feel of the XBMC Foundation website, again, we do not want the visitor to your website to be confused about which company he/she is dealing with.
- Comply with Visual Guidelines - any use of the XBMC Foundation Marks must comply with our Trademark and Logo Usage Policy and our Visual Identity Guidelines at:
    - Visual Guidelines: **Visual Identity Guidelines**
        - Kodi Logos: **Media center logos**
        - XBMC Foundation Logos: **Visual Identity Guidelines**

4 Software Distributions

4.1 Unaltered Binaries

You may distribute unchanged official binaries (i.e., the installer file available for download for each platform (code + config) and not the program executable) downloaded from xbmc.org to anyone in any way, subject to governing law, without receiving any further permission from XBMC Foundation. If you want to distribute the unchanged official binaries using the XBMC Foundation Marks, you may do so, without receiving any further permission from XBMC Foundation, as long as you comply with this Trademark Policy and you distribute them without charge. However, you must not remove or change any part of the official binary, including the XBMC Foundation Marks. On your website or in other materials, you may truthfully state that the software you are providing is an unmodified version of a XBMC Foundation application, keeping in mind the overall guidelines for the use of XBMC Foundation Marks in printed materials, detailed above. We suggest that, if you choose to provide visitors to your website the opportunity to download XBMC Foundation product, you do so by means of a link to our site, to help ensure faster, more reliable downloads.

If you choose to distribute XBMC Foundation binaries yourself, you should make the latest stable version available (of course, you probably want to do so as well). If you compile XBMC Foundation unmodified source code (including code and config files in the installer) and do not charge for it, you do not need additional permission from XBMC Foundation to use the relevant XBMC Foundation Mark(s) for your compiled version. So that users get the latest code and security releases, we encourage you to always distribute the most current official release. The notification requirements of the GNU General Public License have been met for our binaries, so although it's a good idea to do so, you are not required to ship the source code along with the binaries.

In addition, if you are distributing XBMC Foundation binaries yourself, and wish to use the XBMC Foundation Mark(s), you may not (a) disable, modify or otherwise interfere with any installation mechanism contained in a XBMC Foundation product; (b) use any such installation mechanism to install any plug-ins, themes, extensions, software, or items other than the XBMC Foundation product; or (c) use or provide any program, mechanism or process (other than an installation mechanism contained in the XBMC Foundation product) to install such product. Any use of a meta-installer would require our prior written permission.

If you are using the XBMC Foundation Mark(s) for the unaltered binaries you are distributing, you may not charge for that product. By not charging, we mean the XBMC Foundation product must be without cost and its distribution (whether by download or other media) may not be subject to a fee, or tied to subscribing to or purchasing a service, or the collection of personal information. If you want to sell the product, you may do so, but you must call that product by another name—one unrelated to XBMC Foundation or any of the XBMC Foundation Marks (see the sections on "Modifications" and "Related Software" below). Remember that we do not want the public to be confused.

4.2 Modifications

If you're taking full advantage of the open-source nature of XBMC Foundation's products and making significant functional changes, you may not redistribute the fruits of your labor under any XBMC Foundation trademark, without XBMC Foundation's prior written consent. For example, if the product you've modified is Kodi, you may not use XBMC Foundation or Kodi, in whole or in part, in its name. Also, it would be inappropriate for you to say "based on Kodi". Instead, in the interest of complete accuracy, you could describe your executables as "based on Kodi technology", or "incorporating Kodi source code."

In addition, if you compile a modified version, as discussed above, you will require XBMC Foundation's prior written permission. If it's not the unmodified installer package from xbmc.org, and you want to use our trademark(s), our review and approval of your modifications is required. You also must change the name of the executable so as to reduce the chance that a user of the modified software will be misled into believing it to be a native XBMC Foundation product.

Again, any modification to the XBMC Foundation product, including adding to, modifying in any way, or deleting content from the files included with an installer, file location changes, added code, modification of any source files including additions and deletions, etc., will require our permission if you want to use the XBMC Foundation Marks. If you have any doubt, just ask us at contact@kodi.tv

4.3 Add-ons, Skins and other extensions

At the same time as we seek community involvement in the development of the XBMC Foundation products, we want to protect the reputation of these products as high-quality and lightweight, with simple, usable interfaces. If you want to ship add-ons, skins or other extensions installed by default or as part of the same installation process as the XBMC Foundation products, and you plan on distributing them under any XBMC Foundation Marks, you must first seek approval from us. What we find acceptable will depend on the effect of the add-ons, skins and other extensions on the XBMC Foundation product. To give examples, changing the skin of one product to another, equally high-quality and aesthetically pleasing skin would be considered. A combination of various add-ons with intrusive pop-up boxes, with loud and distracting UI sounds, probably wouldn't be. See our **Partners page** to find out more about contacting us to discuss your proposed changes.

4.4 Related Software

XBMC Foundation products are designed to be extended, and we recognize that community members writing add-ons and supplemental software need some way to identify the XBMC Foundation product to which their add-on/software pertain. Our main concern about add-ons and related software is that consumers not be confused as to whether they are official (meaning approved by XBMC Foundation) or not. To address that concern, we request that add-ons and supplemental software names not include, in whole or in part, the words "XBMC Foundation" or "Kodi" in a way that suggests a connection between XBMC Foundation and the add-on or software (e.g., "Frobnicator for Kodi," would be acceptable, but "Kodi Frobnicator" would not).

5 Domain Names

If you want to include all or part of a XBMC Foundation trademark in a domain name, you have to receive written permission from XBMC Foundation. People naturally associate domain names with organizations whose names sound similar. Almost any use of a XBMC Foundation trademark in a domain name is likely to confuse consumers, thus running afoul of the overarching requirement that any use of a XBMC Foundation trademark be non-confusing.

To receive written permission, please download and follow the directions as outlined in the **Domain Name License**.

6 Services Related to XBMC Foundation Software

If you offer services related to XBMC Foundation software, you may use XBMC Foundation's word marks in describing and advertising your services relating to a XBMC Foundation product, so long as you don't violate these overall guidelines for the use of XBMC Foundation's trademarks or do anything that might mislead customers into thinking that either your website, service, or product is a XBMC Foundation website, service, or product, or that XBMC Foundation has any direct relationship with your organization. For example, it's OK if your website says, "Media center customization services for Kodi available here." It's not OK, though, if it says, "Kodi media center customization services sold here," or "custom Kodi media centers available here," since the first suggests that XBMC Foundation is related to your business, and the second is confusing as to whom -- you or XBMC Foundation -- performed the customization. In addition, your website may not copy the look and feel of any XBMC Foundation website. Again, we do not want the visitor to your website to be confused with whom she/he is dealing. When in doubt, err on the side of providing more, rather than less, explanation and information.

If you are offering services for XBMC Foundation software (for example, support), you may not tie the download of the XBMC Foundation product with the purchase of your service. The download of the XBMC Foundation product using the XBMC Foundation trademark may not be connected in any way to the purchase of your service. The purchase, download, or acquisition of your services must be a completely separate transaction from the download of the XBMC Foundation product. You must provide a prominent statement that (i) the XBMC Foundation product is available for free and link directly to our site; (ii) the purchase, download, or acquisition of your service is separate from the download of the XBMC Foundation product; and (iii) your service is not affiliated with XBMC Foundation.

7 XBMC Foundation Marks and Merchandise

When it comes to the XBMC Foundation Marks, there are some cool things you can do and some cool things you can't do - at least not without asking XBMC Foundation.

You may make t-shirts, desktop wallpaper, or baseball caps with XBMC Foundation Marks on them, though only for yourself and your friends (meaning people from whom you don't receive anything of value in return). You can't put the XBMC Foundation Mark(s) on anything that you produce commercially (whether or not you make a profit) -- at least not without receiving XBMC Foundation's written permission. XBMC Foundation contracts with third party vendors that provide XBMC Foundation products for sale.

There is one additional broad category of things you can't do with XBMC Foundation's Marks.

- Produce modified versions of them. A modified mark also would raise the possibility of consumer confusion, thus violating XBMC Foundation's trademark rights (remember the overarching requirement that any use of a XBMC Foundation Mark be non-confusing?).

8 Things You Can Do—Summary

To summarize, provided that the use adheres to our trademark policy and visual guidelines, here are some of the things that you can do with the XBMC Foundation Marks that do not require our permission:

- use the XBMC Foundation Marks in marketing, and other publicity materials related to XBMC Foundation or the relevant XBMC Foundation product;
- distribute unchanged XBMC Foundation product(s) (code + config) for each platform downloaded from xbmc.org as long as you distribute them without charge;
- describe your executables as "based on XBMC Foundation technology", or "incorporating XBMC Foundation source code;"
- link to XBMC Foundation's website(s) to allow your visitors to download Kodi;
- use XBMC Foundation's word marks in describing and advertising your services or products relating to a XBMC Foundation product, so long as you don't do anything that might mislead customers. For example, it's OK if your website says, "Media center customization services for Kodi available here;" and
- make t-shirts, desktop wallpaper, or baseball caps though only for yourself and your friends (meaning people from whom you don't receive anything of value in return).

9 Reporting Trademark Abuse

We have a **central place** for everyone to report any misuse of the XBMC Foundation Marks. All you have to do is fill out the relevant information on the web form. The more information you supply when you file the report, the easier it is for us to evaluate and respond appropriately. Having the support and help of our community makes our work easier and more worthwhile.

10 Questions

We have tried to make our trademark policy as comprehensive as possible. If you're considering a use

of a XBMC Foundation trademark that's not covered by the policy, and you're unsure whether that use would run afoul of XBMC Foundation's guidelines, feel free to contact us at contact@xbmc.org and ask. Please keep in mind that XBMC Foundation receives lots and lots of similar questions, so please review all available documentation, including the **Frequently Asked Questions** (FAQ) before contacting us.

Retrieved from "http://kodi.wiki/view/Official:Trademark_Policy"

Text on this page is available under Attribution-ShareAlike 3.0 Unported. Images and video may be under a different copyright.

Observing Community Anniversaries: 30 years of FSF, 10 years of OIN, 5 years of SFLC.in and their Legal Strategies

Software Freedom Law Center
October 30, 2015

30 years of FSF:

1) Eben Moglen: FSF Legal Strategy in Three Decades

10 years of OIN:

1) Open Invention Network: Open Invention Network Celebrates Its 10 Year Anniversary

2) Roger Parloff, Fortune: Amid the Patent Wars, an Oasis of Calm Collaboration

3) Open Invention Network: OIN License Agreement

5 years of SFLC.in:

1) Supreme Court of India: Writ Petition (Criminal) No.167 of 2012

2) SFLC.in: India's Surveillance State

3) SFLC.in: Information Technology (Intermediaries Guidelines) Rules, 2011; An Analysis

4) SFLC.in: Time-line of Software Patent Law in India

5) Ministry of Communication Information Technology Department of Electronics & Information Technology: Policy on Adoption of Open Source Software for Government of India

FSF Legal Strategy in Three Decades

Eben Moglen

October 2015

THE FREE SOFTWARE FOUNDATION'S THIRTIETH ANNIVERSARY is inevitably a time for looking both backward and forward, as one does in mid-life. Even for a newcomer like me, only twenty-two years in, there is plenty to reflect upon as well as much to imagine. And even newcomers reach the stage at which they realize they ought to write it down just in case: Richard Stallman and I have both led lives as men trying to expect the unexpected, after all.

When and Where: Brief Biographical Background

Richard Stallman and I started working together in 1993. Richard and Jerry Cohen had completed their masterpiece, GPLv2, about eighteen months earlier; LGPLv2, not yet renamed "Lesser," was only slightly younger. I was greatly impressed by what the licenses had achieved, as a bystander, but far less so than I became when I had spent some years working with them. And when Richard first wrote to me asking for help, what he needed had nothing to do with the licenses at all. I told him then, "I use emacs every day, so it will be a long time before you exhaust your entitlement to free legal help from me." Still true.

I spent about eighteen months just answering Richard's questions and doing his legal errands, learning the terrain, before I began to think in terms of shaping a legal strategy for him. In 1994-95, I was teaching at Harvard, so Richard and I saw one another frequently; in after years, more than 16,000 email messages passing between us showed how little time we spent in the same place. We appointed me FSF's General Counsel by mutual consent in 1995, which was as much of an unpaid second job as a newly-tenured young law professor could manage. We worked independently, most of the time connected only by Richard's stream of directing email and my responses. But we did have time to write the GNU Free Document License together at his mother's living-room coffee table in 1999, and to meet in a variety of (mostly Chinese) restaurants in New York, Boston and points farther afield.

In the middle of the Oughts, when we were making GPLv3, we saw one another all the time, working mostly at SFLC's offices in New York, shouting and eating lunch around Lincoln Center. SFLC's acoustics are—I like to think—on a par with the neighborhood catering. The Upper West Side suits us, evidently: we both grew up here, so it can legitimately be considered the Free Software Movement Historic

District, though I'm sure no future mayor of New York City will so designate it. In the space between Lincoln Center and Columbia University, with his mother's apartment placed strategically in the center, Richard and I plotted up the way to turn his absolutely astounding legal invention, the copyleft license, into a functioning system that would catalyze a transformation of software-making everywhere.

What and How: Free Software Legal Strategy

The essence of copyleft is the protection of users' rights. The "copyright bargain" is usually stated as exclusive rights for authors (usually actually meaning the employers or publishers of authors), in return for limited rights of access and use for users. Copyleft fuses both sides of the bargain, employing the exclusive rights granted to authors to broaden enforceable protection for users' rights to learn from, modify, and share.

Strategic Doctrine

Two basic corollaries followed, in my view, from this starting point:

1. The copyright holder is acting on behalf of users in the exercise of his, her or its exclusive statutory rights; and
2. All users must be treated as equally entitled to the benefit of the exercise of the copyright holder's exclusive rights.

The first principle was embodied in the instructions Richard initially gave me about license compliance disputes, in 1994: "Never let a settlement for damages interfere with a settlement for compliance." This properly placed the users' interest in the protection of their rights before the copyright holder's. It also enabled me to open conversations with parties not yet in compliance with the words "we don't want money, or publicity; all we want is compliance, we don't need more and we won't take less."

Because we acted on users' behalf—because my client was committed to the end purpose, and was willing to leave the money on the table so long as our social goal was achieved—our strategy was to maximize compliance, and the perceived credibility of the licenses, at the Foundation's material expense. As history shows, this aspect of the strategy was very successful: all the damages we could ever have collected would not have purchased a small fraction of the credibility GPL earned because our approach placed users' rights ahead of the material interests of the copyright holder.

The second principle, of users' equality in benefit from the license, became a guiding principle of license interpretation. As I learned to understand GPL and LGPL in the 1990s, I was conscious of the importance of treating all users' rights equally, which helped to resolve some issues in when and how to enforce GPL. In our approach to making GPLv3—as Richard and I discussed and reconsidered numerous proposals over the years, and proceeded to do the work in the 2000s—respect for equality of users' rights repeatedly affected our drafting. Not unnecessarily breaking "business

models," or in other words disrupting the real-world practices of users building businesses on free software, was from the outset a crucial objective in interpreting the v2 licenses and designing their successors.

Enforcing License Compliance

At no time did I consider the elimination of copyright infringement on free software to be a credible objective. We were not copyright maximalists, in the first place. The entertainment industries' determination to extirpate every infringer and prevent every technology of infringement represented the antithesis of our beliefs. In the second place, users' rights could only be protected if manufacturers and software integrators chose to use free software in the products: the obvious trade-off between intensity of deterrence and creation of unnecessary fear, uncertainty and doubt had to be resolved against creation of FUD. This was particularly true because an immense, deeply-funded proprietary software monopoly called Microsoft (almost unrecognizable in its contemporary shrunken, palsied state, to which free software competition in due course reduced it) invested very heavily in creating just such fear, uncertainty and doubt among prospective users. Even, therefore, had our resources been adequate to such a Quixotic effort as the elimination of infringement, we would not have undertaken it.

Instead, we were engaged in trust-building. The licenses, and the superb software available on their terms, jointly created a trusted commons. In this copyleft commons, the terms of engagement lent themselves to the attainment of mutual benefit while sharply reducing the risk of competitively advantageous but socially disadvantageous appropriation. Once it was perceived that the rules *could* be enforced without distorting this desirable condition—which it took us most of the 1990s to achieve—parties like IBM and HP, who could knowledgeably evaluate not only the technical value of the software but also the business risks involved in the social practices and legal arrangements involved, became willing to invest heavily in the commons. What mobilized those initial capital commitments was the growth of trust that we had achieved, by making license compliance enforcement credible without departing from the ethical corollaries of Richard's legal invention.

Patents

In early 2006, as we were preparing the first discussion draft of GPLv3 for release, Richard was interviewed by Steve Lohr of the New York Times. "When you started this, Richard, did you ever think free software could get this big?" Steve asked. "No, of course not," Richard immediately replied. "From the moment I first heard about software patenting in the early Nineties, I assumed we were doomed. Eben was more optimistic."

As Richard said, the misapplication of the patent system to software—which began in the United States under the leadership of the late Chief Judge Giles Rich of the Federal Circuit—was an existential threat to the free software movement. Respecting users' rights includes respecting the right to create independently. In copyright, the Supreme Court recognized the constitutional role of the idea/expression distinction

in preventing collision between the First Amendment and Article I, Section 8, which empowers Congress to make patent and copyright laws. But if every particular technique out of thousands or hundreds of thousands employed in the making of one computer program can be exclusively granted to an "owner" for twenty years, the creative reuse and incremental improvement that is the lifeblood of software creation by sharing would be destroyed by the "anticommons" effect of too much ownership.

Our own position, which we articulated as clearly and forcefully as we could, has always been that patent law should not be applied to "inventions" consisting entirely of software running on general purpose computers. We think this was not what Congress intended in making any part of current patent law, and that it inevitably involves grants of property in abstract ideas that the First Amendment does not permit Congress to intend anyway.

But we could not, in my view, base an entire legal strategy on ultimately persuading the Supreme Court that the Federal Circuit could not be entrusted with the future of the global IT industry on the basis of its superior ability to apply patent law to everything. Daniel Ravicher and I appeared as amici curiae in the Supreme Court and in the Federal Circuit whenever we could perceive an opportunity to state our general principle in a fashion with potentially immediate practical effect. We tried to build a body of results *consistent* with our ultimate position. But we needed trust- and coalition-building with parties whose corporate form and long history of patenting precluded them from acting on the basis of our principles.

As very capable patent-getters like IBM and HP began investing in copylefted software and in the social and legal practices that produced it, they began to understand the potential importance of balancing their interests as patentees and licensors with their interests as prosumers of free software. From 2000, we worked intensively across a broad front, with these companies and other coalition partners, to protect free software programs and programmers from the destructive consequences of too much patenting. We established transactional pathways for companies to provide patent assurance to free software programs like GCC. We advised W3C in its pioneering of standards-making that incorporated royalty-free commitments by working group members for recommended technologies. We worked with companies making commitments not to use their patent claims to disrupt free software programs or projects. And we did everything we could to encourage the formation of collective patent security arrangements.

From its creation in 2005, and particularly under the leadership of Keith Bergelt, the Open Invention Network has been our indispensable strategic partner in providing protection against patent aggression from outside the copyleft commons. In 2006-07, Richard and I drafted and negotiated through the public discussion and adoption process GPLv3, the first change in the core copyleft license since 1991. GPLv3 requires parties contributing to licensed programs to provide royalty-free access to all claims practiced by the program version to which they contributed, for that and all future versions and uses of the code.

Between GPLv3's effect within the copyleft commons of each licensed program, and the powerful strategic leadership for broad cross-licensing and collective defense against threats outside the commons provided by OIN, practical defenses and protections against overpatenting have evolved, under our guidance or with our active

support. Our efforts to bring about reconsideration of US patent law, or at least its interpretation by the USPTO and the Federal Circuit, in which we were ultimately joined by many other voices throughout civil society speaking against the ills of over-patenting, have also borne fruit. In a series of cases from *Bilski v. Kappos* to *Alice Corp. v. State Street Bank*, the Supreme Court has, with nearly unbroken unanimity, cut sharply back on the scope of patent with respect to software and "business model inventions" involving the use of general purpose computers and the Internet. We may not have achieved the simplicity of a Supreme Court holding that only a "special purpose machine" or the "transformation of matter" makes software claims patentable, but that is the effective doctrine the cases leave us with, and we can well live with that.

What Now? Future Legal Strategy for Free Software

Having worked in three decades for the legal and political health of free software, I see looking back that some of the future will resemble some of the past. We have trust-building to do again with respect to license compliance. No longer are all copyright holders in copylefted projects adhering to the practices that maximized trust and minimized fear, uncertainty and doubt. We have work to do restoring the understandings that allowed our mechanisms, legal and social, to triumph in the first place.

Our success in achieving safety amidst the dangers of a patent system run a muck has been crucial to our survival, but we are now going to be required to do again with respect to the Chinese patent system what we have done with respect to that of the US—a feat that will be more difficult by far in a system that does not offer apolitical adjudication. The Indian patent system's clear statutory prohibition on patenting software will now again be put in doubt, it appears, by the action of a government that cannot change the law but may wish to change administrative practices in the interests of US multinationals now busily waiving their investment checkbooks. Our institutions of licensing and collective defense will prove their worth many times over, again, in this coming period.

The creation of SFLC in 2005 gave me and my colleagues a chance to coordinate legal strategies for a number of clients, each with their different special situations and interests, beyond the outlook established during the previous decade when I represented only FSF. Looking at free software law now, I see Debian and FreedomBox, along with commercial parties as diverse as Oracle and Canonical, playing roles that FSF would not or cannot play, but contributing valuably and productively to the larger whole. Decades of experience have now accumulated, among project leaders and their lawyers, that will allow us to drive the basic ideas of protecting users' rights more deeply into the society and politics around the world in our Internet Age.

Open Invention Network Celebrates Its 10 Year Anniversary

Link from: https://www.openinventionnetwork.com/pressrelease_details/?id=76

October 06, 2015

The Largest Patent Non-Aggression Organization in History
Reflects on its Achievements and Ongoing Trends

Durham, NC (October 6, 2015) – Open Invention Network (OIN), the largest patent non-aggression community in history, is marking its 10 year anniversary this fall. Since its founding in 2005, Open Invention Network has grown its community to over 1,700 participants – from sizable multinational companies to key open source projects to emerging businesses. OIN has expanded its strategic patent portfolio to more than 1,000 worldwide patents and applications. In parallel, the zone of patent non-aggression that is defined by OIN's Linux System definition has evolved to include more than 2,300 software packages, which ensures freedom of action in core functionality for global open source projects and technology platforms such as Linux, Red Hat, SUSE, Android, Open Stack and Apache.

"Over the past ten years, we have seen explosive growth in open source software, from the enterprise to mobile to the internet of things. The type of collaborative invention that open source drives is yielding higher levels of innovation than ever before, and has demonstrated the power of co-opetition – a balancing of cooperation and competition," said Keith Bergelt, CEO at Open Invention Network. "OIN's approach to patent non-aggression has embraced the notion of co-opetition and ushered in an emerging cultural norm which enables broad based participation in collaborative projects regardless of an organization's perspective on patents while ensuring freedom of action in key Linux and open source technologies."

OIN's community practices patent non-aggression in core Linux and adjacent open source technologies by cross-licensing Linux System patents to one another on a royalty-free basis. Patents owned by Open Invention Network are similarly licensed royalty-free to any organization that agrees not to assert its patents against the Linux System. The OIN license can be signed online at www.j-oin.com.

About Open Invention Network

Open Invention Network (OIN) is the largest patent non-aggression community in history and supports freedom of action in Linux as a key element of open source software. Funded by Google, IBM, NEC, Philips, Red Hat, Sony and SUSE, OIN has more than 1,700 OIN community members and owns more than 1,000 global patents and applications. The OIN patent license and member cross-licenses are available royalty free to any party that joins the OIN community.

For more information, visit http://www.openinventionnetwork.com.

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

©2015 Open Invention Network LLC.

Amid the patent wars, an oasis of calm collaboration

***Available from*: http://fortune.com/2015/10/06/open-invention-network-anniversary/**

by Roger Parloff @rparloff October 6, 2015, 8:42 AM EDT

Ten years ago this week, five public companies—IBM Novell (now SUSE), Philips, Red Hat, and Sony—banded together to launch a novel, pioneering, and seldom heralded project that was one of the first patent defense alliances and, according to some, one of the most successful.

The consortium, known as the Open Invention Network, is dedicated to protecting a mode of collaborative invention. Specifically, it tries to safeguard the Linux open-source software ecosystem—software that's written collaboratively and distributed for free—from patent licensing demands and lawsuits from any aggressor.

OIN's story is an outlier in the recent annals of patent law. It's largely a story about patent peace, not patent war. It's about patent litigations that *haven't* been filed—dogs that haven't barked, basically. It's about otherwise ruthlessly competitive companies laying down their swords in order to cooperate within a narrowly defined space, where they recognize that it's in everyone's best interests to do so.

Originally, the most immediate threat to Linux and open source was Microsoft, whose executives had, in 2001, publicly identified Linux as a "cancer," an "intellectual property-destroyer," and un-American. (In 2007, Microsoft revealed to *Fortune* that it owned 235 patents that it claimed were being infringed by Linux.)

The central mission of OIN—led also, since 2006, by NEC, and, since 2013, by Google—has been described by its CEO, Keith Bergelt, as the provision of a "defensive patent shield" or "no-fly zone" around key open-source software, currently including, among other things, the widely used Linux and Android operating systems for servers, smartphones, and tablets. Such software is favored by more than 90% of Fortune 500 companies for crucial portions of their operations.

OIN's strength lies not just in the financial might and thought-leading influence of its seven sponsoring companies—known as "full members"—but in its ever expanding network of "licensee" companies that sign up to take advantage of the central bargain OIN offers, creating a community that is committed to a corporate ethic of coopetition vis-à-vis software innovation: "Where we cooperate," Bergelt explains, "we're not going to sue each other. Where we compete, however, we compete, and all the normal rules around patenting apply."

"OIN has achieved something I don't know that anybody else has," says Dan McCurdy, "in gathering such a large community of people with the common objective of acting together responsibly to reduce risks. It's quite remarkable." McCurdy is a founder of the nonprofit patent-defense consortium Allied Security Trust, and now works for RPX, a public corporation also devoted to patent defense. Both AST, with 29 member companies, and RPX, which serves 225 subscriber companies, focus on buying

patents before they can be acquired by patent assertion entities—companies, pejoratively known as trolls, which exist to buy patents and sue on them.

OIN is different from RPX or AST. It exists to defend open-source software against any aggressor, including operating companies. Its core function is to buy high-quality, fundamental patents in the realm of, say, e-commerce or information technology, and to hold them in trust for the benefit of the developers, distributors and users of open-source projects. OIN offers to license this treasure trove of patents for free to any user of Linux software who agrees not to assert any of its own patents against the Linux system. Further, OIN pledges to help protect licensees in the event they are named in a patent suit stemming from their use of Linux by, for instance, transferring some of its powerful patents to the licensee for use in a counterclaim against the aggressor. (It made such a transfer to Salesforce.com in 2010, for instance, after the latter was sued by Microsoft. The suit was later settled.)

Though companies were slow to take OIN licenses at first—there were just 32 licensees when Bergelt became CEO in February 2008, 28 months after OIN's launch—the pace has picked up exponentially as norms have taken hold, open-source projects have broadened their footprint, and OIN has expanded its definition of "the Linux system" to keep pace. By the end of 2012 there were more than 500 licensee companies in the OIN network, and today there are close to 1,750, according to Bergelt.

Many OIN licensees are small companies and projects that lack the resources that large companies have to defend themselves against patent aggression. Nevertheless, about 30 public companies have also joined the community as licensees, including giants like Cisco Systems, Fujitsu, HTC, LG Electronics, Nationwide Mutual Insurance Company, Twitter, Verizon, Vodafone, and Yahoo.

The specific, typically behind-the-scenes ways in which OIN pursues its goals have diversified over the years, and are still evolving today.

By its licensing terms, open-source software, whose paradigm is the seminal GNU/Linux operating system developed in 1991, confers certain freedoms on users that are typically denied users of proprietary software, like Microsoft Windows or Apple iOS. These freedoms include the right to see the source code and to freely alter it, copy it, and redistribute it.

Patent claims pose special threats to the open-source ecosystem because, if found to be valid, patent holders can prevent users from exercising any of those freedoms.

Though once thought to be relegated to the realm of hobbyists and hackers, open-source software soon won corporate backers because it was cheap, flexible, and—due to the large community of developers continually making fixes to it—reliable. By the late 1990s key enterprise software vendors, like Oracle, were supporting Linux, as were key server manufacturers, like IBM, Dell and Hewlett-Packard Co.. Red Hat—an early provider of Linux operating systems to corporations—went public in 1999, and SUSE, a German distributor of enterprise Linux software, was acquired by Novell in 2004.

In the summer of 2004, then IBM in-house lawyer Dave Kappos and several colleagues sketched out an architecture for a patent-defense alliance to protect Linux. They then fine-tuned the idea with representatives of the four other companies that would become OIN's other charter members. (Now a partner at Cravath, Swaine & Moore, Kappos served as director of the U.S. Patent and Trademark

Office from 2009 to 2013.)

Commerce One's Crown Jewel Patents

In October 2004, when OIN was still in gestation, the groundbreaking e-commerce company Commerce One filed for bankruptcy—a victim of the dot-com crash. To pay creditors, the company announced that it would auction off its patent portfolio that December, and that Intellectual Ventures, the hedge fund run by polymath and former Microsoft CTO Nathan Myhrvold, had already bid $1 million for it. Since Commerce One's portfolio contained exactly the sort of crown jewel patents the OIN would need for its treasure chest, it was agreed that Novell would acquire them as OIN's stand-in, given that OIN hadn't formally launched yet.

Novell did so—for $15.5 million on the 51st bid—and then contributed the patents to OIN at its formal launch the following October, with the purchase price being offset from its capital contribution. (Though OIN didn't publicly launch until November 2005, the organization views the seeding of the Commerce One portfolio as its operational inception, and dates its anniversaries from then.) Each full OIN member makes a one-time capital contribution, whose size has never been made public by OIN. But Novell's securities filings suggest that, at that time at least, the ante was $20 million. (In 2011 Novell was acquired by Attachmate, with its SUSE unit being spun off. SUSE, now owned by Britain's Micro Focus, has assumed Novell's OIN seat.)

The Commerce One auction turned out to be a signal moment in the development of the secondary market for patents, and also kickstarted the creation of patent-defense alliances, as companies in every sector began to appreciate the danger of letting powerful patents fall into the wrong hands. The auctioneer of the Commerce One portfolio, for example, was John Amster, who, in 2008, went on to found RPX, whose subscribers today include Intel, Ford, Starbucks, and Wells Fargo. (Link free to *Fortune* subscribers only.) One of Novell's competing bidders at the auction was a loose consortium of companies, represented by McCurdy, who, in 2007, formalized their relationship as Allied Security Trust, whose members today include Avaya, Honda, Microsoft, and Oracle. (Some companies—like Google, IBM, and Sony—participate in all three alliances: OIN, AST, and RPX.)

For OIN's first two years its CEO was Jerry Rosenthal, the former head of licensing at IBM. But in February 2008, when it named its successor, it chose Keith Bergelt, who—as a lawyer, diplomat, and businessman—drew on a broader set of skills and experiences, befitting the more diverse role the group envisioned playing.

After earning a law degree from Southern Methodist University, Bergelt, now 57, spent 13 years with the State Department in the foreign service, including a stint in Tokyo. (He speaks French and Japanese.) He left government in 1993 to take courses in business, engineering and telecommunications management at Stanford and the University of San Francisco, before earning an M.B.A. from the technology-focused Theseus Institute in southern France. He then held a series of IP management positions with consulting firms, corporations, and private equity firms, including directing Motorola's IP management and running Paradox Capital, a hedge fund that provides loans secured by IP assets.

Bergelt sees his eclectic training as an eerily perfect fit for his current position. "In the beginning of my career I was making the world safe for democracy," he comments, "while now I really see every day as

advancing the democratization of innovation—allowing people from all around the world to participate in projects and opening up the world to good ideas from wherever they're sourced."

Defensive Publication and Home Grown Patents

Shortly after Bergelt's hiring, OIN began expanding the ways in which it sought to protect the community. In late 2008, it teamed up with the Software Freedom Law Center and The Linux Foundation to launch the Linux Defenders program, under which, among other things, open source developers are urged to submit their inventions for "defensive publication"—an inexpensive way to make sure that no one else can try to patent them.

Since then, OIN has also begun writing patent applications of its own, both to expand the utility of the patents it has purchased and also "to invent based on where the market is going, and where technology is moving," Bergelt explains.

Today OIN owns about 650 issued patents and another 350 patent applications. Of the issued patents, he says, about 125 are "home grown," as are about 200 of the applications.

Bergelt, on OIN's behalf, also sometimes lobbies lawmakers on bills of concern to the community, and meets with antitrust regulators to discuss large patent deals or other events that could threaten the community's interests.

As Linux expanded its functionality, OIN has continually expanded its definition of the Linux system to encompass more software packages. Today, Linux provides the operating systems embedded inside most cameras; TVs; remotely controlled thermostats and the like (dubbed the Internet of Things); and an increasing number of automotive navigational and infotainment systems. It has become the software of choice for supercomputing, mathematical modeling, and weather prediction, and is widely used in the burgeoning field of cloud computing. And thanks to Google's Android and Chrome, of course, it also now drives more than 80% of smartphones and a large percentage of tablets and notebooks.

To keep up , OIN now covers 2,300 software "packages," including core portions of both Android and OpenStack, which is a set of projects relating to cloud computing. "Other than Linux, Open Stack will probably be viewed in hindsight as the most significant open-source project in history," says Bergelt, citing the importance of the inventions, the number of participants (more than 500 companies), and the amount of code being written.

OIN's champions measure its success by the success of Linux and the large number of licensees who now participate in the OIN network. On the other hand, given how opaque the world of patent licensing is, it's hard to prove or quantify OIN's impact.

Florian Mueller, an IP analyst who founded the FOSSPatents blog, is profoundly skeptical of OIN's value. In an email he asserts, "The OIN does not have any solid proof of concept. It's more of a myth and a mystery." (Mueller consults for private companies, and his past clients have included Microsoft and Oracle.)

Mueller points out, for instance, that most of the manufacturers of Android phones—including OIN

licensees HTC and LG—have taken licenses to Microsoft's patent portfolio for the right to ship Android. Microsoft's large and diverse portfolio includes, Microsoft claims, patents that read on Linux functionality. (The *Wall Street Journal* reported last year that Samsung—which is not an OIN licensee—was paying Microsoft more than $1 billion in annual patent royalties for the right to sell Android smartphones. Microsoft declined to comment for any aspect of this article.)

Bergelt says that OIN's success does not hinge on whether some OIN participants decide in the end to pay patent license royalties to patent holders. "We're not trying to prevent people from doing what they think is prudent," he says. "That doesn't stop us from working behind the scenes to reduce the effect of these patents that are yielding royalties right now, in so far as they support an anti-innovation agenda."

He adds: "Android's Linux component has not been sued and never will be as long as OIN continues to facilitate patent non-aggression within the parameters of the Linux system." Rather, Bergelt insists, "the suits [that have been filed] have been over applications agnostic to the operating system and Linux," which ride higher up in the software stack.

OIN has suffered some setbacks in recent years as five sizable OIN licensees have withdrawn after joining: Oracle (which withdrew in March 2012); Geeknet (November 2012); HP (August 2013); Facebook (August 2013); and Symantec (October 2013). Asked about these incidents, Bergelt says that the only reason a company would do this is to reserve the right to bring a suit relating to functionality included in the Linux system, which casts doubt on these companies' commitment to open source. "The litmus test for authenticity in open source . . . is becoming an OIN signatory," he says. "Companies that either elect not to become signatories or shed the obligations of an OIN license . . . are making a clear statement regarding their authenticity."

Oracle and Symantec declined comment both as to why they withdrew and on Bergelt's statement. The other three companies did not respond to inquiries seeking comment.

Still, open-source projects unquestionably look to OIN for both protection and guidance. In recent years, Bergelt says, OIN has been "nurturing micro-clusters of patent non-aggression pacts," in which specific open-source projects use OIN as a model for coopetition. Though these groups do not acquire patents, as OIN does, they do attempt to draw frontiers—at a more granular level than OIN can—about where participants will cooperate and where they will compete.

To this end, for instance, Bergelt has met with the AllSeen Alliance, which pursues open-source projects relating to the Internet of Things, and with a group within The Clearing House payments company, owned by the 24 largest global banks, which promotes the development of open-source financial software resistant to cyber attack.

"It's a great model," says Sean Reilly, senior vice president and associate general counsel for The Clearing House. "Everyone jumps in to collaborate together for the common plumbing," he continues. "But then the other lane is hypercompetitive, and you can do what you like with your intellectual property rights."

Bergelt acknowledges that OIN plays a modest role, and is only "part of a larger mosaic" in the open-source world. The real credit goes to "the people who take the risk of building a business based on open

source," like a Red Hat, or those who take "left turns," like IBM did in the late 1990s, when it began committing hundreds of millions of dollars to supporting Linux.

"We're there to have a light touch," he says. "To guide, shape, protect, and guard—but not to leave an imprint."

© 2015 Time Inc. All rights reserved.

Fortune.com is a part of the Time.com network of sites.

OIN License Agreement

Link from: https://www.openinventionnetwork.com/joining-oin/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.

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

©2015 Open Invention Network LLC.

REPORTABLE

IN THE SUPREME COURT OF INDIA

CRIMINAL/CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CRIMINAL) NO.167 OF 2012

SHREYA SINGHAL … PETITIONER

VERSUS

UNION OF INDIA … RESPONDENT

WITH

WRIT PETITION (CIVIL) NO.21 OF 2013

WRIT PETITION (CIVIL) NO.23 OF 2013

WRIT PETITION (CIVIL) NO. 97 OF 2013

WRIT PETITION (CRIMINAL) NO.199 OF 2013

WRIT PETITION (CIVIL) NO. 217 OF 2013

WRIT PETITION (CRIMINAL) NO.222 OF 2013

WRIT PETITION (CRIMINAL) NO.225 OF 2013

WRIT PETITION (CIVIL) NO.758 OF 2014

WRIT PETITION (CRIMINAL) NO.196 OF 2014

J U D G M E N T

R.F. NARIMAN, J.

1. This batch of writ petitions filed under Article 32 of the Constitution of India raises very important and far-reaching questions relatable primarily to the fundamental right of free speech and expression guaranteed by Article 19(1)(a) of the Constitution of India. The immediate cause for concern in these petitions is Section 66A of the Information Technology Act of 2000. This Section was not in the Act as originally enacted, but came into force by virtue of an Amendment Act of 2009 with effect from 27.10.2009. Since all the arguments raised by several counsel for the petitioners deal with the unconstitutionality of this Section it is set out hereinbelow:

> "**66-A. Punishment for sending offensive messages through communication service, etc**. —Any person who sends, by means of a computer resource or a communication device,—
>
> (*a*) any information that is grossly offensive or has menacing character; or
>
> (*b*) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such

computer resource or a communication device; or

(*c*) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation.— For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message."[1]

1

The genealogy of this Section may be traced back to Section 10(2)(a) of the U.K. Post Office (Amendment) Act, 1935, which made it an offence to send any message by telephone which is grossly offensive or of an indecent, obscene, or menacing character. This Section was substantially reproduced by Section 66 of the UK Post Office Act, 1953 as follows:

66. Prohibition of sending offensive or false telephone messages or false telegrams, etc.

If any person—

(a)sends any message by telephone which is grossly offensive or of an indecent, obscene or menacing character ;

(b)sends any message by telephone, or any telegram, which he knows to be false, for the purpose of causing annoyance, inconvenience or needless anxiety to any other person ; or

(c)persistently makes telephone calls without reasonable cause and for any such purpose as aforesaid,

he shall be liable on summary conviction to a fine not exceeding ten pounds, or to imprisonment for a term not exceeding one month, or to both.

This Section in turn was replaced by Section 49 of the British Telecommunication Act, 1981 and Section 43 of the British Telecommunication Act, 1984. In its present form in the UK, it is Section 127 of the Telecommunication Act, 2003 which is relevant and which is as follows:-

127. Improper use of public electronic communications network

(1) A person is guilty of an offence if he -

(a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or

(b) cause any such message or matter to be so sent.

2. A related challenge is also made to Section 69A introduced by the same amendment which reads as follows:-

> **"69-A. Power to issue directions for blocking for public access of any information through any computer resource**.—(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.
>
> (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

---

(2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he-

(a) sends by means of a public electronic communications network, a message that he knows to be false,

(b) causes such a message to be sent; or

(c) persistently makes use of a public electronic communications network.

(3) A person guilty of an offence under this section shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale, or to both.

(4) Subsections (1) and (2) do not apply to anything done in the course of providing a programme service (within the meaning of the Broadcasting Act 1990 (c.42)).

> (3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine."

3. The Statement of Objects and Reasons appended to the Bill which introduced the Amendment Act stated in paragraph 3 that:

> "3. A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal code, the Indian Evidence Act and the code of Criminal Procedure to prevent such crimes."

4. The petitioners contend that the very basis of Section 66A - that it has given rise to new forms of crimes - is incorrect, and that Sections 66B to 67C and various Sections of the Indian Penal Code (which will be referred to hereinafter) are good enough to deal with all these crimes.

5. The petitioners' various counsel raised a large number of points as to the constitutionality of Section 66A. According to them, first and foremost Section 66A infringes the fundamental right to free speech and expression and is not saved by any of the eight subjects covered in Article 19(2). According to them, the causing of annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill-will are all outside the purview of Article 19(2). Further, in creating an offence, Section 66A suffers from the vice of vagueness because unlike the offence created by Section 66 of the same Act, none of the aforesaid terms are even attempted to be defined and cannot be defined, the result being that innocent persons are roped in as well as those who are not. Such persons are not told clearly on which side of the line they fall; and it would be open to the authorities to be as arbitrary and whimsical as they like in booking such persons under the said Section. In fact, a large number of innocent persons have been booked and many instances have been given in the form of a note to the Court. The enforcement of the said Section would really be an insidious form of censorship which impairs a core

value contained in Article 19(1)(a). In addition, the said Section has a chilling effect on the freedom of speech and expression. Also, the right of viewers is infringed as such chilling effect would not give them the benefit of many shades of grey in terms of various points of view that could be viewed over the internet.

The petitioners also contend that their rights under Articles 14 and 21 are breached inasmuch there is no intelligible differentia between those who use the internet and those who by words spoken or written use other mediums of communication. To punish somebody because he uses a particular medium of communication is itself a discriminatory object and would fall foul of Article 14 in any case.

6. In reply, Mr. Tushar Mehta, learned Additional Solicitor General defended the constitutionality of Section 66A. He argued that the legislature is in the best position to understand and appreciate the needs of the people. The Court will, therefore, interfere with the legislative process only when a statute is clearly violative of the rights conferred on the citizen

under Part-III of the Constitution. There is a presumption in favour of the constitutionality of an enactment. Further, the Court would so construe a statute to make it workable and in doing so can read into it or read down the provisions that are impugned. The Constitution does not impose impossible standards of determining validity. Mere possibility of abuse of a provision cannot be a ground to declare a provision invalid. Loose language may have been used in Section 66A to deal with novel methods of disturbing other people's rights by using the internet as a tool to do so. Further, vagueness is not a ground to declare a statute unconstitutional if the statute is otherwise legislatively competent and non-arbitrary. He cited a large number of judgments before us both from this Court and from overseas to buttress his submissions.

Freedom of Speech and Expression

Article 19(1)(a) of the Constitution of India states as follows:

> "**Article 19. Protection of certain rights regarding freedom of speech, etc.**—(1) All citizens shall have the right—
> (*a*) to freedom of speech and expression;"

7. Article 19(2) states:

> **"Article 19. Protection of certain rights regarding freedom of speech, etc.**—(2) Nothing in sub-clause (*a*) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence."

8. The Preamble of the Constitution of India *inter alia* speaks of liberty of thought, expression, belief, faith and worship. It also says that India is a sovereign democratic republic. It cannot be over emphasized that when it comes to democracy, liberty of thought and expression is a cardinal value that is of paramount significance under our constitutional scheme.

9. Various judgments of this Court have referred to the importance of freedom of speech and expression both from the point of view of the liberty of the individual and from the point of view of our democratic form of government. For example, in

the early case of **Romesh Thappar** v. **State of Madras,** [1950] S.C.R. 594 at 602, this Court stated that freedom of speech lay at the foundation of all democratic organizations. In **Sakal Papers (P) Ltd. & Ors.** v. **Union of India,** [1962] 3 S.C.R. 842 at 866, a Constitution Bench of this Court said freedom of speech and expression of opinion is of paramount importance under a democratic constitution which envisages changes in the composition of legislatures and governments and must be preserved. In a separate concurring judgment Beg,J. said, in **Bennett Coleman & Co. & Ors. v. Union of India & Ors**., [1973] 2 S.C.R. 757 at 829, that the freedom of speech and of the press is the Ark of the Covenant of Democracy because public criticism is essential to the working of its institutions.[2]

10. Equally, in **S. Khushboo** v. **Kanniamal & Anr.**, (2010) 5 SCC 600 this Court stated, in paragraph 45 that the importance of freedom of speech and expression though not absolute was

---

2

Incidentally, the Ark of the Covenant is perhaps the single most important focal point in Judaism. The original ten commandments which the Lord himself gave to Moses was housed in a wooden chest which was gold plated and called the Ark of the Covenant and carried by the Jews from place to place until it found its final repose in the first temple - that is the temple built by Solomon.

necessary as we need to tolerate unpopular views. This right requires the free flow of opinions and ideas essential to sustain the collective life of the citizenry. While an informed citizenry is a pre-condition for meaningful governance, the culture of open dialogue is generally of great societal importance.

11. This last judgment is important in that it refers to the "market place of ideas" concept that has permeated American Law. This was put in the felicitous words of Justice Holmes in his famous dissent in **Abrams v. United States,** 250 US 616 (1919), thus:

> "But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas-that the best test of truth is the power of thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution."

12. Justice Brandeis in his famous concurring judgment in **Whitney** v. **California,** 71 L. Ed. 1095 said:

“Those who won our independence believed that the final end of the state was to make men free to develop their faculties, and that in its government the deliberative forces should prevail over the arbitrary. They valued liberty both as an end and as a means. They believed liberty to be the secret of happiness and courage to be the secret of liberty. They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth; that without free speech and assembly discussion would be futile; that with them, discussion affords ordinarily adequate protection against the dissemination of noxious doctrine; that the greatest menace to freedom is an inert people; that public discussion is a political duty; and that this should be a fundamental principle of the American government. They recognized the risks to which all human institutions are subject. But they knew that order cannot be secured merely through fear of punishment for its infraction; that it is hazardous to discourage thought, hope and imagination; that fear breeds repression; that repression breeds hate; that hate menaces stable government; that the path of safety lies in the opportunity to discuss freely supposed grievances and proposed remedies; and that the fitting remedy for evil counsels is good ones. Believing in the power of reason as applied through public discussion, they eschewed silence coerced by law-the argument of force in its worst form. Recognizing the occasional tyrannies of governing majorities, they amended the Constitution so that free speech and assembly should be guaranteed.

Fear of serious injury cannot alone justify suppression of free speech and assembly. Men feared witches and burnt women. It is the function of speech to free men from the bondage of irrational fears. To justify suppression of free speech there must be reasonable ground to fear that serious evil will result if free speech is practiced. There must be reasonable ground to believe that the danger apprehended is imminent. There must be reasonable ground to believe that the evil to be prevented is a serious one. Every denunciation of existing law tends in some measure to increase the probability that there will be violation of it. Condonation of a breach enhances the probability. Expressions of approval add to the probability. Propagation of the criminal state of mind by teaching syndicalism increases it. Advocacy of lawbreaking heightens it still further. But even advocacy of violation, however reprehensible morally, is not a justification for denying free speech where the advocacy falls short of incitement and there is nothing to indicate that the advocacy would be immediately acted on. The wide difference between advocacy and incitement, between preparation and attempt, between assembling and conspiracy, must be borne in mind. In order to support a finding of clear and present danger it must be shown either that immediate serious violence was to be expected or was advocated, or that the past conduct furnished reason to believe that such advocacy was then contemplated." (at page 1105, 1106)

13. This leads us to a discussion of what is the content of the expression "freedom of speech and expression". There are three concepts which are fundamental in understanding the reach of this most basic of human rights. The first is discussion, the second is advocacy, and the third is incitement. Mere discussion or even advocacy of a particular cause howsoever unpopular is at the heart of Article 19(1)(a). It is only when such discussion or advocacy reaches the level of incitement that Article 19(2) kicks in.[3] It is at this stage that a law may be made curtailing the speech or expression that leads

3

A good example of the difference between advocacy and incitement is Mark Antony's speech in Shakespeare's immortal classic Julius Caesar. Mark Antony begins cautiously. Brutus is chastised for calling Julius Caesar ambitious and is repeatedly said to be an "honourable man". He then shows the crowd Caesar's mantle and describes who struck Caesar where. It is at this point, after the interjection of two citizens from the crowd, that Antony says-

"ANTONY- Good friends, sweet friends, let me not stir you up
To such a sudden flood of mutiny.
They that have done this deed are honourable:
What private griefs they have, alas, I know not,
That made them do it: they are wise and honourable,
And will, no doubt, with reasons answer you.
I come not, friends, to steal away your hearts:
I am no orator, as Brutus is;
But, as you know me all, a plain blunt man,
That love my friend; and that they know full well
That gave me public leave to speak of him:
For I have neither wit, nor words, nor worth,
Action, nor utterance, nor the power of speech,
To stir men's blood: I only speak right on;
I tell you that which you yourselves do know;
Show you sweet Caesar's wounds, poor poor dumb mouths,
And bid them speak for me: but were I Brutus,
And Brutus Antony, there were an Antony
Would ruffle up your spirits and put a tongue
In every wound of Caesar that should move
The stones of Rome to rise and mutiny.
ALL- We'll mutiny."

inexorably to or tends to cause public disorder or tends to cause or tends to affect the sovereignty & integrity of India, the security of the State, friendly relations with foreign States, etc. Why it is important to have these three concepts in mind is because most of the arguments of both petitioners and respondents tended to veer around the expression "public order".

14. It is at this point that a word needs to be said about the use of American judgments in the context of Article 19(1)(a). In virtually every significant judgment of this Court, reference has been made to judgments from across the Atlantic. Is it safe to do so?

15. It is significant to notice first the differences between the US First Amendment and Article 19(1)(a) read with Article 19(2). The first important difference is the absoluteness of the U.S. first Amendment – Congress shall make <u>no law</u> which abridges the freedom of speech. Second, whereas the U.S. First Amendment speaks of freedom of speech and of the press, without any reference to "expression", Article 19(1)(a) speaks of

freedom of speech and expression without any reference to "the press". Third, under the US Constitution, speech may be abridged, whereas under our Constitution, reasonable restrictions may be imposed. Fourth, under our Constitution such restrictions have to be in the interest of eight designated subject matters - that is any law seeking to impose a restriction on the freedom of speech can only pass muster if it is proximately related to any of the eight subject matters set out in Article 19(2).

16. Insofar as the first apparent difference is concerned, the U.S. Supreme Court has never given literal effect to the declaration that Congress shall make no law abridging the freedom of speech. The approach of the Court which is succinctly stated in one of the early U.S. Supreme Court Judgments, continues even today. In **Chaplinsky** v. **New Hampshire,** 86 L. Ed. 1031, Justice Murphy who delivered the opinion of the Court put it thus:-

> "Allowing the broadest scope to the language and purpose of the Fourteenth Amendment, it is well understood that the right of free speech is not

> absolute at all times and under all circumstances. There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which has never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words—those which by their very utterance inflict injury or tend to incite an immediate breach of the peace. It has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality. 'Resort to epithets or personal abuse is not in any proper sense communication of information or opinion safeguarded by the Constitution, and its punishment as a criminal act would raise no question under that instrument.' Cantwell v. Connecticut, 310 U.S. 296, 309, 310, 60 S.Ct. 900, 906, 84 L.Ed.1213, 128 A.L.R. 1352." (at page 1035)

17. So far as the second apparent difference is concerned, the American Supreme Court has included "expression" as part of freedom of speech and this Court has included "the press" as being covered under Article 19(1)(a), so that, as a matter of judicial interpretation, both the US and India protect the freedom of speech and expression as well as press freedom. Insofar as abridgement and reasonable restrictions are concerned, both the U.S. Supreme Court and this Court have

held that a restriction in order to be reasonable must be narrowly tailored or narrowly interpreted so as to abridge or restrict only what is absolutely necessary. It is only when it comes to the eight subject matters that there is a vast difference. In the U.S., if there is a compelling necessity to achieve an important governmental or societal goal, a law abridging freedom of speech may pass muster. But in India, such law cannot pass muster if it is in the interest of the general public. Such law has to be covered by one of the eight subject matters set out under Article 19(2). If it does not, and is outside the pale of 19(2), Indian courts will strike down such law.

18. Viewed from the above perspective, American judgments have great persuasive value on the content of freedom of speech and expression and the tests laid down for its infringement. It is only when it comes to sub-serving the general public interest that there is the world of a difference. This is perhaps why in **Kameshwar Prasad & Ors.** v. **The State of Bihar & Anr.,** 1962 Supp. (3) S.C.R. 369, this Court held:

> "As regards these decisions of the American Courts, it should be borne in mind that though the First Amendment to the Constitution of the United State reading "Congress shall make no law.... abridging the freedom of speech..." appears to confer no power on the Congress to impose any restriction on the exercise of the guaranteed right, still it has always been understood that the freedom guaranteed is subject to the police power - the scope of which however has not been defined with precision or uniformly. It is on the basis of the police power to abridge that freedom that the constitutional validity of laws penalising libels, and those relating to sedition, or to obscene publications etc., has been sustained. The resultant flexibility of the restrictions that could be validly imposed renders the American decisions inapplicable to and without much use for resolving the questions arising under Art. 19(1) (a) or (b) of our Constitution wherein the grounds on which limitations might be placed on the guaranteed right are set out with definiteness and precision." (At page 378)

19. But when it comes to understanding the impact and content of freedom of speech, in **Indian Express Newspapers (Bombay) Private Limited & Ors.** v. **Union of India & Ors.,** (1985) 2 SCR 287, Venkataramiah,J. stated:

> "While examining the constitutionality of a law which is alleged to contravene Article 19 (1) (a) of the Constitution, we cannot, no doubt, be solely guided by the decisions of the Supreme Court of the United States of America. But in order to understand the basic principles of freedom of speech and expression and the need for that freedom in a

> democratic country, we may take them into consideration. The pattern of Article 19 (1) (a) and of Article 19 (1) (g) of our constitution is different from the pattern of the First Amendment to the American Constitution which is almost absolute in its terms. The rights guaranteed under Article 19 (1) (a) and Article 19 (1) (g) of the Constitution are to be read along with clauses (2) and (6) of Article 19 which carve out areas in respect of which valid legislation can be made." (at page 324)

20. With these prefatory remarks, we will now go to the other aspects of the challenge made in these writ petitions and argued before us.

A. <u>Article 19(1)(a)</u> –

Section 66A has been challenged on the ground that it casts the net very wide – "all information" that is disseminated over the internet is included within its reach. It will be useful to note that Section 2(v) of Information Technology Act, 2000 defines information as follows:

> "2. **Definitions**.—(1) In this Act, unless the context otherwise requires,—
> (v) "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche."

Two things will be noticed. The first is that the definition is an inclusive one. Second, the definition does not refer to what the content of information can be. In fact, it refers only to the medium through which such information is disseminated. It is clear, therefore, that the petitioners are correct in saying that the public's right to know is directly affected by Section 66A. Information of all kinds is roped in – such information may have scientific, literary or artistic value, it may refer to current events, it may be obscene or seditious. That such information may cause annoyance or inconvenience to some is how the offence is made out. It is clear that the right of the people to know – the market place of ideas – which the internet provides to persons of all kinds is what attracts Section 66A. That the information sent has to be annoying, inconvenient, grossly offensive etc., also shows that no distinction is made between mere discussion or advocacy of a particular point of view which may be annoying or inconvenient or grossly offensive to some and incitement by which such words lead to an imminent causal connection with public disorder, security of State etc. The petitioners are right in saying that Section 66A in creating an

offence against persons who use the internet and annoy or cause inconvenience to others very clearly affects the freedom of speech and expression of the citizenry of India at large in that such speech or expression is directly curbed by the creation of the offence contained in Section 66A.

In this regard, the observations of Justice Jackson in **American Communications Association** v. **Douds**, 94 L. Ed. 925 are apposite:

> "Thought control is a copyright of totalitarianism, and we have no claim to it. It is not the function of our Government to keep the citizen from falling into error; it is the function of the citizen to keep the Government from falling into error. We could justify any censorship only when the censors are better shielded against error than the censored."

B. <u>Article 19(2)</u>

One challenge to Section 66A made by the petitioners' counsel is that the offence created by the said Section has no proximate relation with any of the eight subject matters contained in Article 19(2). We may incidentally mention that the State has claimed that the said Section can be supported under

the heads of public order, defamation, incitement to an offence and decency or morality.

21. Under our constitutional scheme, as stated earlier, it is not open to the State to curtail freedom of speech to promote the general public interest. In **Sakal Papers (P) Ltd. & Ors. v. Union of India,** [1962] 3 S.C.R. 842, this Court said:

> "It may well be within the power of the State to place, in the interest of the general public, restrictions upon the right of a citizen to carry on business but it is not open to the State to achieve this object by directly and immediately curtailing any other freedom of that citizen guaranteed by the Constitution and which is not susceptible of abridgment on the same grounds as are set out in clause (6) of Article 19. Therefore, the right of freedom of speech cannot be taken away with the object of placing restrictions on the business activities of a citizen. Freedom of speech can be restricted only in the interests of the security of the State, friendly relations with foreign State, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence. It cannot, like the freedom to carry on business, be curtailed in the interest of the general public. If a law directly affecting it is challenged, it is no answer that the restrictions enacted by it are justifiable under clauses (3) to (6). For, the scheme of Article 19 is to enumerate different freedoms separately and then to specify the extent of restrictions to which they may be subjected and the objects for securing which this could be done. A citizen is entitled to

> enjoy each and every one of the freedoms together and clause (1) does not prefer one freedom to another. That is the plain meaning of this clause. It follows from this that the State cannot make a law which directly restricts one freedom even for securing the better enjoyment of another freedom. All the greater reason, therefore for holding that the State cannot directly restrict one freedom by placing an otherwise permissible restriction on another freedom." (at page 863)

22. Before we come to each of these expressions, we must understand what is meant by the expression "in the interests of". In **The Superintendent, Central Prison, Fatehgarh** v. **Ram Manohar Lohia,** [1960] 2 S.C.R. 821, this Court laid down:

> "We do not understand the observations of the Chief Justice to mean that any remote or fanciful connection between the impugned Act and the public order would be sufficient to sustain its validity. The learned Chief Justice was only making a distinction between an Act which expressly and directly purported to maintain public order and one which did not expressly state the said purpose but left it to be implied there from; and between an Act that directly maintained public order and that indirectly brought about the same result. <u>The distinction does not ignore the necessity for intimate connection between the Act and the public order sought to be maintained by the Act</u>." (at pages 834, 835)
>
> "The restriction made "in the interests of public order" must also have reasonable relation to the

> object to be achieved, i.e., the public order. If the restriction has no proximate relationship to the achievement of public order, it cannot be said that the restriction is a reasonable restriction within the meaning of the said clause." (at page 835)
>
> "The decision, in our view, lays down the correct test. The limitation imposed in the interests of public order to be a reasonable restriction, should be one which has a proximate connection or nexus with public order, but not one far-fetched, hypothetical or problematical or too remote in the chain of its relation with the public order.....There is no proximate or even foreseeable connection between such instigation and the public order sought to be protected under section. We cannot accept the argument of the learned Advocate General that instigation of a single individual not to pay tax or dues is a spark which may in the long run ignite a revolutionary movement destroying public order" (at page 836).

Reasonable Restrictions:

23. This Court has laid down what "reasonable restrictions" means in several cases. In **Chintaman Rao v. The State of Madhya Pradesh,** [1950] S.C.R. 759, this Court said:

> "The phrase "reasonable restriction" connotes that the limitation imposed on a person in enjoyment of the right should not be arbitrary or of an excessive nature, beyond what is required in the interests of the public. The word "reasonable" implies intelligent care and deliberation, that is, the choice of a course which reason dictates.

> Legislation which arbitrarily or excessively invades the right cannot be said to contain the quality of reasonableness and unless it strikes a proper balance between the freedom guaranteed in article 19(1)(g) and the social control permitted by clause (6) of article 19, it must be held to be wanting in that quality." (at page 763)

24. In **State of Madras v. V.G. Row,** [1952] S.C.R. 597, this Court said:

> "This Court had occasion in Dr. Khare's case (1950) S.C.R. 519 to define the scope of the judicial review under clause (5) of Article19 where the phrase "imposing reasonable restriction on the exercise of the right" also occurs and four out of the five Judges participating in the decision expressed the view (the other Judge leaving the question open) that both the substantive and the procedural aspects of the impugned restrictive law should be examined from the point of view of reasonableness; that is to say, the Court should consider not only factors such as the duration and the extent of the restrictions, but also the circumstances under which and the manner in which their imposition has been authorised. It is important in this context to bear in mind that the test of reasonableness, where ever prescribed, should be applied to each, individual statute impugned and no abstract standard, or general pattern of reasonableness can be laid down as applicable to all cases. The nature of the right alleged to have been infringed, the underlying purpose of the restriction imposed, the extent and urgency of the evil sought to be remedied thereby, the disproportion of the imposition, the prevailing conditions at the time, should all enter into the judicial verdict. In evaluating such elusive factors

and forming their own conception of what is reasonable, in all the circumstances of a given case, it is inevitable that the social philosophy and the scale of values of the judges participating in the decision should play an important part, and the limit to their interference with legislative judgment in such cases can only be dictated by their sense of responsibility and self- restraint and the sobering reflection that the Constitution is meant not only for people of their way of thinking but for all, and that the majority of the elected representatives of the people have, in authorising the imposition of the restrictions, considered them to be reasonable." (at page 606-607)

25. Similarly, in **Mohd. Faruk v. State of Madhya Pradesh & Ors.**, [1970] 1 S.C.R. 156, this Court said:

"The Court must in considering the validity of the impugned law imposing a prohibition on the carrying on of a business or profession, attempt an evaluation of its direct and immediate impact upon the fundamental rights of the citizens affected thereby and the larger public interest sought to be ensured in the light of the object sought to be achieved, the necessity to restrict the citizen's freedom, the inherent pernicious nature of the act prohibited or its capacity or tendency to be harmful to the general public, the possibility of achieving the object by imposing a less drastic restraint, and in the absence of exceptional situations such as the prevalence of a state of emergency-national or local-or the necessity to maintain essential supplies, or the necessity to stop activities inherently dangerous, the existence of a machinery to satisfy the administrative authority that no case for

> imposing the restriction is made out or that a less drastic restriction may ensure the object intended to be achieved." (at page 161)

26. In **Dr. N. B. Khare** v. **State of Delhi,** [1950] S.C.R. 519, a Constitution Bench also spoke of reasonable restrictions when it comes to procedure. It said:

> "While the reasonableness of the restrictions has to be considered with regard to the exercise of the right, it does not necessarily exclude from the consideration of the Court the question of reasonableness of the procedural part of the law. It is obvious that if the law prescribes five years externment or ten years externment, the question whether such period of externment is reasonable, being the substantive part, is necessarily for the consideration of the court under clause (5). Similarly, if the law provides the procedure under which the exercise of the right may be restricted, the same is also for the consideration of the Court, as it has to determine if the exercise of the right has been reasonably restricted." (at page 524)

27. It was argued by the learned Additional Solicitor General that a relaxed standard of reasonableness of restriction should apply regard being had to the fact that the medium of speech being the internet differs from other mediums on several grounds. To appreciate the width and scope of his

submissions, we are setting out his written submission verbatim:

> "(i) the reach of print media is restricted to one state or at the most one country while internet has no boundaries and its reach is global;
>
> (ii) the recipient of the free speech and expression used in a print media can only be literate persons while internet can be accessed by literate and illiterate both since one click is needed to download an objectionable post or a video;
>
> (iii) In case of televisions serials [except live shows] and movies, there is a permitted pre-censorship' which ensures right of viewers not to receive any information which is dangerous to or not in conformity with the social interest. While in the case of an internet, no such pre-censorship is possible and each individual is publisher, printer, producer, director and broadcaster of the content without any statutory regulation;
>
> (iv) In case of print media or medium of television and films whatever is truly recorded can only be published or broadcasted I televised I viewed. While in case of an internet, morphing of images, change of voices and many other technologically advance methods to create serious potential social disorder can be applied.
>
> (v) By the medium of internet, rumors having a serious potential of creating a serious social disorder can be spread to trillions of people without any check which is not possible in case of other mediums.
>
> (vi) In case of mediums like print media, television and films, it is broadly not possible to invade privacy of

unwilling persons. While in case of an internet, it is very easy to invade upon the privacy of any individual and thereby violating his right under Article 21 of the Constitution of India.

(vii) By its very nature, in the mediums like newspaper, magazine, television or a movie, it is not possible to sexually harass someone, outrage the modesty of anyone, use unacceptable filthy language and evoke communal frenzy which would lead to serious social disorder. While in the case of an internet, it is easily possible to do so by a mere click of a button without any geographical limitations and almost in all cases while ensuring anonymity of the offender.

(viii) By the very nature of the medium, the width and reach of internet is manifold as against newspaper and films. The said mediums have inbuilt limitations i.e. a person will have to buy / borrow a newspaper and / or will have to go to a theater to watch a movie. For television also one needs at least a room where a television is placed and can only watch those channels which he has subscribed and that too only at a time where it is being telecast. While in case of an internet a person abusing the internet, can commit an offence at any place at the time of his choice and maintaining his anonymity in almost all cases.

(ix) In case of other mediums, it is impossible to maintain anonymity as a result of which speech ideal opinions films having serious potential of creating a social disorder never gets generated since its origin is bound to be known. While in case of an internet mostly its abuse takes place under the garb of anonymity which can be unveiled only after thorough investigation.

(x) In case of other mediums like newspapers, television or films, the approach is always institutionalized approach governed by industry

> specific ethical norms of self conduct. Each newspaper / magazine / movie production house / TV Channel will have their own institutionalized policies in house which would generally obviate any possibility of the medium being abused. As against that use of internet is solely based upon individualistic approach of each individual without any check, balance or regulatory ethical norms for exercising freedom of speech and expression under Article 19[1] [a].
>
> (xi) In the era limited to print media and cinematograph; or even in case of publication through airwaves, the chances of abuse of freedom of expression was less due to inherent infrastructural and logistical constrains. In the case of said mediums, it was almost impossible for an individual to create and publish an abusive content and make it available to trillions of people. Whereas, in the present internet age the said infrastructural and logistical constrains have disappeared as any individual using even a smart mobile phone or a portable computer device can create and publish abusive material on its own, without seeking help of anyone else and make it available to trillions of people by just one click."

28. As stated, all the above factors may make a distinction between the print and other media as opposed to the internet and the legislature may well, therefore, provide for separate offences so far as free speech over the internet is concerned. There is, therefore, an intelligible differentia having a rational relation to the object sought to be achieved – that there can be

creation of offences which are applied to free speech over the internet alone as opposed to other mediums of communication. Thus, an Article 14 challenge has been repelled by us on this ground later in this judgment. But we do not find anything in the features outlined by the learned Additional Solicitor General to relax the Court's scrutiny of the curbing of the content of free speech over the internet. While it may be possible to narrowly draw a Section creating a new offence, such as Section 69A for instance, relatable only to speech over the internet, yet the validity of such a law will have to be tested on the touchstone of the tests already indicated above.

29. In fact, this aspect was considered in **Secretary Ministry of Information & Broadcasting, Government of India** v. **Cricket Association of Bengal**, (1995) 2 SCC 161 in para 37, where the following question was posed:

> "The next question which is required to be answered is whether there is any distinction between the freedom of the print media and that of the electronic media such as radio and television, and if so, whether it necessitates more restrictions on the latter media."

This question was answered in para 78 thus:

> "There is no doubt that since the airwaves/frequencies are a public property and are also limited, they have to be used in the best interest of the society and this can be done either by a central authority by establishing its own broadcasting network or regulating the grant of licences to other agencies, including the private agencies. What is further, the electronic media is the most powerful media both because of its audio-visual impact and its widest reach covering the section of the society where the print media does not reach. The right to use the airwaves and the content of the programmes, therefore, needs regulation for balancing it and as well as to prevent monopoly of information and views relayed, which is a potential danger flowing from the concentration of the right to broadcast/telecast in the hands either of a central agency or of few private affluent broadcasters. That is why the need to have a central agency representative of all sections of the society free from control both of the Government and the dominant influential sections of the society. This is not disputed. But to contend that on that account the restrictions to be imposed on the right under Article 19(1)(*a*) should be in addition to those permissible under Article 19(2) and dictated by the use of public resources in the best interests of the society at large, is to misconceive both the content of the freedom of speech and expression and the problems posed by the element of public property in, and the alleged scarcity of, the frequencies as well as by the wider reach of the media. <u>If the right to freedom of speech and expression includes the right to disseminate information to as wide a section of the population as is possible, the access which enables the right to be so exercised is also an integral part of the said right. The wider range of</u>

circulation of information or its greater impact cannot restrict the content of the right nor can it justify its denial. The virtues of the electronic media cannot become its enemies. It may warrant a greater regulation over licensing and control and vigilance on the content of the programme telecast. However, this control can only be exercised within the framework of Article 19(2) and the dictates of public interests. To plead for other grounds is to plead for unconstitutional measures. It is further difficult to appreciate such contention on the part of the Government in this country when they have a complete control over the frequencies and the content of the programme to be telecast. They control the sole agency of telecasting. They are also armed with the provisions of Article 19(2) and the powers of pre-censorship under the Cinematograph Act and Rules. The only limitation on the said right is, therefore, the limitation of resources and the need to use them for the benefit of all. When, however, there are surplus or unlimited resources and the public interests so demand or in any case do not prevent telecasting, the validity of the argument based on limitation of resources disappears. It is true that to own a frequency for the purposes of broadcasting is a costly affair and even when there are surplus or unlimited frequencies, only the affluent few will own them and will be in a position to use it to subserve their own interest by manipulating news and views. That also poses a danger to the freedom of speech and expression of the have-nots by denying them the truthful information on all sides of an issue which is so necessary to form a sound view on any subject. That is why the doctrine of fairness has been evolved in the US in the context of the private broadcasters licensed to share the limited frequencies with the central agency like the FCC to regulate the programming. But this phenomenon occurs even in the case of the print media of all the

> countries. Hence the body like the Press Council of India which is empowered to enforce, however imperfectly, the right to reply. The print media further enjoys as in our country, freedom from pre-censorship unlike the electronic media."

Public Order

30. In Article 19(2) (as it originally stood) this sub-head was conspicuously absent. Because of its absence, challenges made to an order made under Section 7 of the Punjab Maintenance of Public Order Act and to an order made under Section 9 (1)(a) of the Madras Maintenance of Public Order Act were allowed in two early judgments by this Court. Thus in **Romesh Thappar** v. **State of Madras,** [1950] S.C.R. 594, this Court held that an order made under Section 9(1)(a) of the Madras Maintenance of Public Order Act (XXIII of 1949) was unconstitutional and void in that it could not be justified as a measure connected with security of the State. While dealing with the expression "public order", this Court held that "public order" is an expression which signifies a state of tranquility which prevails amongst the members of a political society as a result of the internal regulations enforced by the Government which they have established.

31. Similarly, in **Brij Bhushan & Anr.** v. **State of Delhi**, [1950] S.C.R. 605, an order made under Section 7 of the East Punjab Public Safety Act, 1949, was held to be unconstitutional and void for the self-same reason.

32. As an aftermath of these judgments, the Constitution First Amendment added the words “public order” to Article 19(2).

33. In **Superintendent, Central Prison, Fatehgarh** v. **Ram Manohar Lohia,** [1960] 2 S.C.R. 821, this Court held that public order is synonymous with public safety and tranquility; it is the absence of disorder involving breaches of local significance in contradistinction to national upheavals, such as revolution, civil strife, war, affecting the security of the State. This definition was further refined in **Dr. Ram Manohar Lohia** v. **State of Bihar & Ors.,** [1966] 1 S.C.R. 709, where this Court held:

> “It will thus appear that just as "public order" in the rulings of this Court (earlier cited) was said to comprehend disorders of less gravity than those

> affecting "security of State", "law and order" also comprehends disorders of less gravity than those affecting "public order". One has to imagine three concentric circles. Law and order represents the largest circle within which is the next circle representing public order and the smallest circle represents security of State. It is then easy to see that an act may affect law and order but not public order just as an act may affect public order but not security of the State." (at page 746)

34. In **Arun Ghosh** v. **State of West Bengal,** [1970] 3 S.C.R. 288, **Ram Manohar Lohia's case** was referred to with approval in the following terms:

> "In Dr. Ram Manohar Lohia's case this Court pointed out the difference between maintenance of law and order and its disturbance and the maintenance of public order and its disturbance. Public order was said to embrace more of the community than law and order. Public order is the even tempo of the life of the community taking the country as a whole or even a specified locality. Disturbance of public order is to be distinguished, from acts directed against individuals which do not disturb the society to the extent of causing a general disturbance of public tranquility. It is the degree of disturbance and its effect upon the life of the community in a locality which determines whether the disturbance amounts only to a breach of law and order. Take for instance, a man stabs another. People may be shocked and even disturbed, but the life of the community keeps moving at an even tempo, however much one may dislike the act. Take another case of a town where there is communal tension. A man stabs a member of the other

community. This is an act of a very different sort. Its implications are deeper and it affects the even tempo of life and public order is jeopardized because the repercussions of the act embrace large Sections of the community and incite them to make further breaches of the law and order and to subvert the public order. An act by itself is not determinant of its own gravity. In its quality it may not differ from another but in its potentiality it may be very different. Take the case of assault on girls. A guest at a hotel may kiss or make advances to half a dozen chamber maids. He may annoy them and also the management but he does not cause disturbance of public order. He may even have a fracas with the friends of one of the girls but even then it would be a case of breach of law and order only. Take another case of a man who molests women in lonely places. As a result of his activities girls going to colleges and schools are in constant danger and fear. Women going for their ordinary business are afraid of being waylaid and assaulted. The activity of this man in its essential quality is not different from the act of the other man but in its potentiality and in its effect upon the public tranquility there is a vast difference. The act of the man who molests the girls in lonely places causes a disturbance in the even tempo of living which is the first requirement of public order. He disturbs the society and the community. His act makes all the women apprehensive of their honour and he can be said to be causing disturbance of public order and not merely committing individual actions which may be taken note of by the criminal prosecution agencies. It means therefore that the question whether a man has only committed a breach of law and order or has acted in a manner likely to cause a disturbance of the public order is a question of degree and the extent of the reach of the act upon the society. The French distinguish law and order and public order by designating the latter as order publique. The

> latter expression has been recognised as meaning something more than ordinary maintenance of law and order. Justice Ramaswami in Writ Petition No. 179 of 1968 drew a line of demarcation between the serious and aggravated forms of breaches of public order which affect the community or endanger the public interest at large from minor breaches of peace which do not affect the public at large. He drew an analogy between public and private crimes. The analogy is useful but not to be pushed too far. A large number of acts directed against persons or individuals may total up into a breach of public order. In Dr. Ram Manohar Lohia's case examples were given by Sarkar, and Hidayatullah, JJ. They show how similar acts in different contexts affect differently law and order on the one hand and public order on the other. It is always a question of degree of the harm and its effect upon the community. The question to ask is: Does it lead to disturbance of the current of life of the community so as to amount to a disturbance of the public order or does it affect merely an individual leaving the tranquility of the society undisturbed? This question has to be faced in every case on facts. There is no formula by which one case can be distinguished from another." (at pages 290 and 291).

35. This decision lays down the test that has to be formulated in all these cases. We have to ask ourselves the question: does a particular act lead to disturbance of the current life of the community or does it merely affect an individual leaving the tranquility of society undisturbed? Going by this test, it is clear that Section 66A is intended to punish any person who uses the

internet to disseminate any information that falls within the sub-clauses of Section 66A. It will be immediately noticed that the recipient of the written word that is sent by the person who is accused of the offence is not of any importance so far as this Section is concerned. (Save and except where under sub-clause (c) the addressee or recipient is deceived or misled about the origin of a particular message.) It is clear, therefore, that the information that is disseminated may be to one individual or several individuals. The Section makes no distinction between mass dissemination and dissemination to one person. Further, the Section does not require that such message should have a clear tendency to disrupt public order. Such message need not have any potential which could disturb the community at large. The nexus between the message and action that may be taken based on the message is conspicuously absent – there is no ingredient in this offence of inciting anybody to do anything which a reasonable man would then say would have the tendency of being an immediate threat to public safety or tranquility. On all these counts, it is clear that the Section has no proximate relationship to public order

whatsoever. The example of a guest at a hotel `annoying' girls is telling – this Court has held that mere `annoyance' need not cause disturbance of public order. Under Section 66A, the offence is complete by sending a message for the purpose of causing annoyance, either `persistently' or otherwise without in any manner impacting public order.

Clear and present danger – tendency to affect.

36. It will be remembered that Justice Holmes in **Schenck** v. **United States,** 63 L. Ed. 470 enunciated the clear and present danger test as follows:

> "…The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic. It does not even protect a man from an injunction against uttering words that may have all the effect of force. Gompers v. Buck's Stove & Range Co., 221 U. S. 418, 439, 31 Sup. Ct. 492, 55 L. ed. 797, 34 L. R. A. (N. S.) 874. The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent. It is a question of proximity and degree." (At page 473, 474)

37. This was further refined in **Abrams** v. **Unites States** 250 U.S. 616 (1919), this time in a Holmesian dissent, to be clear

and imminent danger. However, in most of the subsequent judgments of the U.S. Supreme Court, the test has been understood to mean to be "clear and present danger". The test of "clear and present danger" has been used by the U.S. Supreme Court in many varying situations and has been adjusted according to varying fact situations. It appears to have been repeatedly applied, see- **Terminiello** v. **City of Chicago** 93 L. Ed. 1131 (1949) at page 1134-1135, **Brandenburg** v. **Ohio** 23 L. Ed. 2d 430 (1969) at 434-435 & 436, **Virginia** v. **Black** 155 L. Ed. 2d 535 (2003) at page 551, 552 and 553[4].

4

In its present form the clear and present danger test has been reformulated to say that:

"The constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action."

Interestingly, the US Courts have gone on to make a further refinement. The State may ban what is called a "true threat".

"'True threats' encompass those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals."

"The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats protects individuals from the fear of violence and from the disruption that fear engenders, in addition to protecting people from the possibility that the threatened violence will occur. Intimidation in the constitutionally proscribable sense of the word is a type of true threat, where a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death."

See Virginia v. Black (Supra) and Watts v. United States 22 L. Ed. 2d. 664 at 667

38. We have echoes of it in our law as well **S. Rangarajan** v. **P. Jagjivan & Ors.,** (1989) 2 SCC 574 at paragraph 45:

> "45. The problem of defining the area of freedom of expression when it appears to conflict with the various social interests enumerated under Article 19(2) may briefly be touched upon here. There does indeed have to be a compromise between the interest of freedom of expression and special interests. But we cannot simply balance the two interests as if they are of equal weight. Our commitment of freedom of expression demands that it cannot be suppressed unless the situations created by allowing the freedom are pressing and the community interest is endangered. The anticipated danger should not be remote, conjectural or far-fetched. It should have proximate and direct nexus with the expression. The expression of thought should be intrinsically dangerous to the public interest. In other words, the expression should be inseparably locked up with the action contemplated like the equivalent of a "spark in a powder keg".

39. This Court has used the expression "tendency" to a particular act. Thus, in **State of Bihar** v. **Shailabala Devi,** [1952] S.C.R. 654, an early decision of this Court said that an article, in order to be banned must have a tendency to excite persons to acts of violence (at page 662-663). The test laid down in the said decision was that the article should be considered as a whole in a fair free liberal spirit and then it must

be decided what effect it would have on the mind of a reasonable reader. (at pages 664-665)

40. In **Ramji Lal Modi** v. **The State of U.P.,** [1957] S.C.R. 860 at page 867, this court upheld Section 295A of the Indian Penal Code only because it was read down to mean that aggravated forms of insults to religion must have a tendency to disrupt public order. Similarly, in **Kedar Nath Singh** v. **State of Bihar,** 1962 Supp. (2) S.C.R. 769, Section 124A of the Indian Penal Code was upheld by construing it narrowly and stating that the offence would only be complete if the words complained of have a tendency of creating public disorder by violence. It was added that merely creating disaffection or creating feelings of enmity in certain people was not good enough or else it would violate the fundamental right of free speech under Article 19(1)(a). Again, in **Dr. Ramesh Yeshwant Prabhoo** v. **Prabhakar Kashinath Kunte & Ors.,** 1996 (1) SCC 130, Section 123 (3A) of the Representation of People Act was upheld only if the enmity or hatred that was spoken

about in the Section would tend to create immediate public disorder and not otherwise.

41. Viewed at either by the standpoint of the clear and present danger test or the tendency to create public disorder, Section 66A would not pass muster as it has no element of any tendency to create public disorder which ought to be an essential ingredient of the offence which it creates.

Defamation

42. Defamation is defined in Section 499 of the Penal Code as follows:

> "499. **Defamation.**—Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.
>
> *Explanation 1*.—It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

> *Explanation 2*.—It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.
>
> *Explanation 3*.—An imputation in the form of an alternative or expressed ironically, may amount to defamation.
>
> *Explanation 4*.—No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful."

43. It will be noticed that for something to be defamatory, injury to reputation is a basic ingredient. Section 66A does not concern itself with injury to reputation. Something may be grossly offensive and may annoy or be inconvenient to somebody without at all affecting his reputation. It is clear therefore that the Section is not aimed at defamatory statements at all.

<u>Incitement to an offence</u>:

44. Equally, Section 66A has no proximate connection with incitement to commit an offence. Firstly, the information disseminated over the internet need not be information which "incites" anybody at all. Written words may be sent that may be purely in the realm of "discussion" or "advocacy" of a "particular point of view". Further, the mere causing of annoyance, inconvenience, danger etc., or being grossly offensive or having a menacing character are not offences under the Penal Code at all. They may be ingredients of certain offences under the Penal Code but are not offences in themselves. For these reasons, Section 66A has nothing to do with "incitement to an offence". As Section 66A severely curtails information that may be sent on the internet based on whether it is grossly offensive, annoying, inconvenient, etc. and being unrelated to any of the eight subject matters under Article 19(2) must, therefore, fall foul of Article 19(1)(a), and not being saved under Article 19(2), is declared as unconstitutional.

Decency or Morality

45. This Court in **Ranjit Udeshi** v. **State of Maharashtra** [1965] 1 S.C.R. 65 took a rather restrictive view of what would pass muster as not being obscene. The Court followed the test laid down in the old English judgment in **Hicklin's case** which was whether the tendency of the matter charged as obscene is to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall. Great strides have been made since this decision in the UK, United States as well as in our country. Thus, in **Director General, Directorate General of Doordarshan** v. **Anand Patwardhan**, 2006 (8) SCC 433, this Court noticed the law in the United States and said that a material may be regarded as obscene if the average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest and that taken as a whole it otherwise lacks serious literary artistic, political, educational or scientific value (see Para 31).

46. In a recent judgment of this Court, **Aveek Sarkar** v. **State of West Bengal,** 2014 (4) SCC 257, this Court referred to

English, U.S. and Canadian judgments and moved away from the Hicklin test and applied the contemporary community standards test.

47. What has been said with regard to public order and incitement to an offence equally applies here. Section 66A cannot possibly be said to create an offence which falls within the expression ‘decency’ or ‘morality’ in that what may be grossly offensive or annoying under the Section need not be obscene at all – in fact the word ‘obscene’ is conspicuous by its absence in Section 66A.

48. However, the learned Additional Solicitor General asked us to read into Section 66A each of the subject matters contained in Article 19(2) in order to save the constitutionality of the provision. We are afraid that such an exercise is not possible for the simple reason that when the legislature intended to do so, it provided for some of the subject matters contained in Article 19(2) in Section 69A. We would be doing complete violence to the language of Section 66A if we were to

read into it something that was never intended to be read into it.

Further, he argued that the statute should be made workable, and the following should be read into Section 66A:

> "(i) Information which would appear highly abusive, insulting, pejorative, offensive by reasonable person in general, judged by the standards of an open and just multi-caste, multi-religious, multi racial society;
>
> - **Director of Public Prosecutions v. Collins – (2006) 1 WLR 2223** @ para 9 and 21
> - **Connolly v. Director of Public Prosecutions** reported in [2008] 1 W.L.R. 276/2007 [1] All ER 1012
> - House of Lords Select Committee 1st Report of Session 2014-2015 on Communications titled as "Social Media And Criminal Offences" @ pg 260 of compilation of judgments Vol I Part B
>
> (ii) Information which is directed to incite or can produce imminent lawless action **Brandenburg v. Ohio 395 U.S. 444 (1969);**
>
> (iii) Information which may constitute credible threats of violence to the person or damage;
>
> (iv) Information which stirs the public to anger, invites violent disputes brings about condition of violent unrest and disturbances;
> ***Terminiello v. Chicago 337 US 1 (1949)***
>
> (v) Information which advocates or teaches the duty, necessity or proprietary of violence as a means of accomplishing political, social or religious reform and/or justifies commissioning of violent acts with an intent to exemplify glorify such violent means to

accomplish political, social, economical or religious reforms
[Whitney vs. California 274 US 357];

(vi) Information which contains fighting or abusive material;
Chaplinsky v. New Hampshire, 315 U.S. 568 (1942)

(vii) Information which promotes hate speech i.e.

(a) Information which propagates hatred towards individual or a groups, on the basis of race, religion, religion, casteism, ethnicity,

(b) Information which is intended to show the supremacy of one particular religion/race/caste by making disparaging, abusive and/or highly inflammatory remarks against religion/race/caste.

(c) Information depicting religious deities, holy persons, holy symbols, holy books which are created to insult or to show contempt or lack of reverence for such religious deities, holy persons, holy symbols, holy books or towards something which is considered sacred or inviolable.

(viii) Satirical or iconoclastic cartoon and caricature which fails the test laid down in ***Hustler Magazine, Inc. v. Falwell 485 U.S. 46 (1988)***

(ix) Information which glorifies terrorism and use of drugs;

(x) Information which infringes right of privacy of the others and includes acts of cyber bullying, harassment or stalking.

> (xi) Information which is obscene and has the tendency to arouse feeling or revealing an overt sexual desire and should be suggestive of deprave mind and designed to excite sexual passion in persons who are likely to see it.
> ***Aveek Sarkar and Anr. vs. State of West Bengal and Ors.*** *(2014) 4 SCC 257.*
>
> (xii) Context and background test of obscenity. Information which is posted in such a context or background which has a consequential effect of outraging the modesty of the pictured individual.
> ***Aveek Sarkar and Anr. vs. State of West Bengal and Ors.*** *(2014) 4 SCC 257."*

49. What the learned Additional Solicitor General is asking us to do is not to read down Section 66A – he is asking for a wholesale substitution of the provision which is obviously not possible.

Vagueness

50. Counsel for the petitioners argued that the language used in Section 66A is so vague that neither would an accused person be put on notice as to what exactly is the offence which has been committed nor would the authorities administering the Section be clear as to on which side of a clearly drawn line a particular communication will fall.

51. We were given Collin's dictionary, which defined most of the terms used in Section 66A, as follows:

"Offensive:-

1. Unpleasant or disgusting, as to the senses
2. Causing anger or annoyance; insulting
3. For the purpose of attack rather than defence.

Menace:-

1. To threaten with violence, danger, etc.
2. A threat of the act of threatening
3. Something menacing; a source of danger
4. A nuisance

Annoy:-

1. To irritate or displease
2. To harass with repeated attacks

Annoyance

1. The feeling of being annoyed
2. The act of annoying.

Inconvenience

1. The state of quality of being inconvenient
2. Something inconvenient; a hindrance, trouble, or difficulty

Danger:-

1. The state of being vulnerable to injury, loss, or evil risk
2. A person or a thing that may cause injury pain etc.

Obstruct:-

1. To block (a road a passageway, etc.) with an obstacle
2. To make (progress or activity) difficult.
3. To impede or block a clear view of.

Obstruction:- a person or a thing that obstructs.

Insult:-

1. To treat, mention, or speak to rudely; offend; affront
2. To assault; attack
3. An offensive or contemptuous remark or action; affront; slight
4. A person or thing producing the effect of an affront = some television is an insult to intelligence
5. An injury or trauma."

52. The U.S. Supreme Court has repeatedly held in a series of judgments that where no reasonable standards are laid down to define guilt in a Section which creates an offence, and where no clear guidance is given to either law abiding citizens or to authorities and courts, a Section which creates an offence and which is vague must be struck down as being arbitrary and unreasonable. Thus, in **Musser** v. **Utah**, 92 L. Ed. 562, a Utah statute which outlawed conspiracy to commit acts injurious to public morals was struck down.

53. In **Winters** v. **People of State of New York,** 92 L. Ed. 840, a New York Penal Law read as follows:-

"1141. Obscene prints and articles

> 1. A person……who,
>
> 2. Prints, utters, publishes, sells, lends, gives away, distributes or shows, or has in his possession with intent to sell, lend, give away, distribute or show, or otherwise offers for sale, loan, gift or distribution, any book, pamphlet, magazine, newspaper or other printed paper devoted to the publication, and principally made up of criminal news, police reports, or accounts of criminal deeds, or pictures, or stories of deeds of bloodshed, lust or crime; ……..
>
> 'Is guilty of a misdemeanor, …..'" (at page 846)

The court in striking down the said statute held:

> "The impossibility of defining the precise line between permissible uncertainty in statutes caused by describing crimes by words well understood through long use in the criminal law - obscene, lewd, lascivious, filthy, indecent or disgusting—and the unconstitutional vagueness that leaves a person uncertain as to the kind of prohibited conduct—massing stories to incite crime—has resulted in three arguments of this case in this Court. The legislative bodies in draftsmanship obviously have the same difficulty as do the judicial in interpretation. Nevertheless despite the difficulties, courts must do their best to determine whether or not the vagueness is of such a character 'that men of common intelligence must necessarily guess at its meaning.' Connally v. General Constr. Co., 269 U.S. 385, 391, 46 S.Ct. 126, 127, 70 L.Ed. 322. The entire text of the statute or the subjects dealt with may furnish an adequate standard. The present case as to a vague statute abridging free speech

involves the circulation of only vulgar magazines. The next may call for decision as to free expression of political views in the light of a statute intended to punish subversive activities.

The subsection of the New York Penal Law, as now interpreted by the Court of Appeals prohibits distribution of a magazine principally made up of criminal news or stories of deeds of bloodshed, or lust, so massed as to become vehicles for inciting violent and depraved crimes against the person. But even considering the gloss put upon the literal meaning by the Court of Appeals' restriction of the statute to collections of stories 'so massed as to become vehicles for inciting violent and depraved crimes against the person * * * not necessarily * * * sexual passion,' we find the specification of publications, prohibited from distribution, too uncertain and indefinite to justify the conviction of this petitioner. Even though all detective tales and treatises on criminology are not forbidden, and though publications made up of criminal deeds not characterized by bloodshed or lust are omitted from the interpretation of the Court of Appeals, we think fair use of collections of pictures and stories would be interdicted because of the utter impossibility of the actor or the trier to know where this new standard of guilt would draw the line between the allowable and the forbidden publications. No intent or purpose is required—no indecency or obscenity in any sense heretofore known to the law. 'So massed as to incite to crime' can become meaningful only by concrete instances. This one example is not enough. The clause proposes to punish the printing and circulation of publications that courts or juries may think influence generally persons to commit crime of violence against the person. No conspiracy to commit a crime is required. See Musser v. State of Utah, 68 S.Ct. 397, this Term. It is not an effective notice of new crime.

> The clause has no technical or common law meaning. Nor can light as to the meaning be gained from the section as a whole or the Article of the Penal Law under which it appears. As said in the Cohen Grocery Co. case, supra, 255 U.S. at page 89, 41 S.Ct. at page 300, 65 L.Ed. 516, 14 A.L.R. 1045:
>
> 'It leaves open, therefore, the widest conceivable inquiry, the scope of which no one can foresee and the result of which no one can foreshadow or adequately guard against.'
>
> The statute as construed by the Court of Appeals does not limit punishment to the indecent and obscene, as formerly understood. When stories of deeds of bloodshed, such as many in the accused magazines, are massed so as to incite to violent crimes, the statute is violated. it does not seem to us that an honest distributor of publications could know when he might be held to have ignored such a prohibition. Collections of tales of war horrors, otherwise unexceptionable, might well be found to be 'massed' so as to become 'vehicles for inciting violent and depraved crimes.' Where a statute is so vague as to make criminal an innocent act, a conviction under it cannot be sustained. Herndon v. Lowry, 301 U.S. 242, 259, 57 S.Ct. 732, 739, 81 L.Ed. 1066." (at page 851-852)

54. In **Burstyn** v. **Wilson,** 96 L. Ed. 1098, sacrilegious writings and utterances were outlawed. Here again, the U.S. Supreme Court stepped in to strike down the offending Section stating:

> "It is not a sufficient answer to say that 'sacrilegious' is definite, because all subjects that in any way might be interpreted as offending the religious beliefs of any one of the 300 sects of the United States are banned in New York. To allow such vague, undefinable powers of censorship to be exercised is bound to have stultifying consequences on the creative process of literature and art—for the films are derived largely from literature. History does not encourage reliance on the wisdom and moderation of the censor as a safeguard in the exercise of such drastic power over the minds of men. We not only do not know but cannot know what is condemnable by 'sacrilegious.' And if we cannot tell, how are those to be governed by the statute to tell? (at page 1121)

55. In **City of Chicago** v. **Morales et al**, 527 U.S. 41 (1999), a Chicago Gang Congregation Ordinance prohibited criminal street gang members from loitering with one another or with other persons in any public place for no apparent purpose. The Court referred to an earlier judgment in **United States** v. **Reese** 92 U.S. 214 (1875) at 221 in which it was stated that <u>the Constitution does not permit a legislature to set a net large enough to catch all possible offenders and leave it to the Court to step in and say who could be rightfully detained and who should be set at liberty</u>. It was held that the broad sweep of the Ordinance violated the requirement that a legislature needs to

meet: to establish minimum guidelines to govern law enforcement. As the impugned Ordinance did not have any such guidelines, a substantial amount of innocent conduct would also be brought within its net, leading to its unconstitutionality.

56. It was further held that a penal law is void for vagueness if it fails to define the criminal offence with sufficient definiteness. Ordinary people should be able to understand what conduct is prohibited and what is permitted. Also, those who administer the law must know what offence has been committed so that arbitrary and discriminatory enforcement of the law does not take place.

57. Similarly, in **Grayned** v. **City of Rockford,** 33 L.Ed. 2d. 222, the State of Illinois provided in an anti noise ordinance as follows:

> "'(N)o person, while on public or private grounds adjacent to any building in which a school or any class thereof is in session, shall willfully make or assist in the making of any noise or diversion which disturbs or tends to disturb the peace or good order

> of such school session or class thereof. . . .' Code of Ordinances, c. 28, § 19.2(a).”

The law on the subject of vagueness was clearly stated thus:

> “It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined. Vague laws offend several important values. First, because we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. Third, but related, where a vague statute 'abut(s) upon sensitive areas of basic First Amendment freedoms,-it ‘operates to inhibit the exercise of (those) freedoms.’ Uncertain meanings inevitably lead citizens to "steer far wider of the unlawful zone' . . . than if the boundaries of the forbidden areas were clearly marked.'”(at page 227-228)

58. The anti noise ordinance was upheld on facts in that case because it fixed the time at which noise disrupts school activity

– while the school is in session – and at a fixed place – 'adjacent' to the school.

59. Secondly, there had to be demonstrated a causality between disturbance that occurs and the noise or diversion. Thirdly, acts have to be willfully done. It is important to notice that the Supreme Court specifically held that "undesirables" or their "annoying conduct" may not be punished. It is only on these limited grounds that the said Ordinance was considered not to be impermissibly vague.

60. In **Reno**, **Attorney General of the United States, et al.** v. **American Civil Liberties Union et al.,** 521 U.S. 844 (1997), two provisions of the Communications Decency Act of 1996 which sought to protect minors from harmful material on the internet were adjudged unconstitutional. This judgment is a little important for two basic reasons – that it deals with a penal offence created for persons who use the internet as also for the reason that the statute which was adjudged unconstitutional uses the expression "patently offensive" which comes extremely

close to the expression “grossly offensive” used by the impugned Section 66A. Section 223(d), which was adjudged unconstitutional, is set out hereinbelow:-

> “223 (d) Whoever—
>
> “(1) in interstate or foreign communications knowingly—
>
> (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or
>
> (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, “any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or
>
> (2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,
>
> shall be fined under Title 18, or imprisoned not more than two years, or both.” (at page 860)

Interestingly, the District Court Judge writing of the internet said:

> "[i]t is no exaggeration to conclude that the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country – and indeed the world – as yet seen. The plaintiffs in these actions correctly describe the 'democratizing' effects of Internet communication: individual citizens of limited means can speak to a worldwide audience on issues of concern to them. Federalists and Anti-federalists may debate the structure of their government nightly, but these debates occur in newsgroups or chat rooms rather than in pamphlets. Modern-day Luthers still post their theses, but to electronic bulletins boards rather than the door of the Wittenberg Schlosskirche. More mundane (but from a constitutional perspective, equally important) dialogue occurs between aspiring artists, or French cooks, or dog lovers, or fly fishermen." 929 F. Supp. At 881. (at page 425)

61. The Supreme Court held that the impugned statute lacked the precision that the first amendment required when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the impugned Act effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another.

62. Such a burden on adult speech is unacceptable if less restrictive alternatives would be as effective in achieving the legitimate purpose that the statute was enacted to serve. It was held that the general undefined term "patently offensive" covers large amounts of non-pornographic material with serious educational or other value and was both vague and over broad.

It was, thus, held that the impugned statute was not narrowly tailored and would fall foul of the first amendment.

63. In **Federal Communications Commission** v. **Fox Television Stations**, 132 S.Ct. 2307, it was held:

> "A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required. See *Connally* v. *General Constr. Co.*, 269 U. S. 385, 391 (1926) ("[A] statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law"); *Papachristou* v. *Jacksonville*, 405 U. S. 156, 162 (1972) ("Living under a rule of law entails various suppositions, one of which is that '[all persons] are entitled to be informed as to what the State commands or forbids'" (quoting *Lanzetta* v. *New Jersey*, 306 U. S. 451, 453 (1939) (alteration in original))). This requirement of clarity in regulation is

> essential to the protections provided by the Due Process Clause of the Fifth Amendment. See *United States* v. *Williams*, 553 U. S. 285, 304 (2008). It requires the invalidation of laws that are impermissibly vague. A conviction or punishment fails to comply with due process if the statute or regulation under which it is obtained "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *Ibid.* As this Court has explained, a regulation is not vague because it may at times be difficult to prove an incriminating fact but rather because it is unclear as to what fact must be proved. See *id.*, at 306.
>
> Even when speech is not at issue, the void for vagueness doctrine addresses at least two connected but discrete due process concerns: first, that regulated parties should know what is required of them so they may act accordingly; second, precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way. See *Grayned* v. *City of Rockford*, 408 U. S. 104, 108–109 (1972). When speech is involved, rigorous adherence to those requirements is necessary to ensure that ambiguity does not chill protected speech."(at page 2317)

64. Coming to this Court's judgments, in **State of Madhya Pradesh** v. **Baldeo Prasad,** [1961] 1 S.C.R. 970 an inclusive definition of the word "goonda" was held to be vague and the offence created by Section 4A of the Goondas Act was,

therefore, violative of Article 19(1)(d) and (e) of the Constitution.

It was stated:

> "Incidentally it would also be relevant to point out that the definition of the word "goonda" affords no assistance in deciding which citizen can be put under that category. It is an inclusive definition and it does not indicate which tests have to be applied in deciding whether a person falls in the first part of the definition. Recourse to the dictionary meaning of the word would hardly be of any assistance in this matter. After all it must be borne in mind that the Act authorises the District Magistrate to deprive a citizen of his fundamental right under Art. 19(1)(d) and (e), and though the object of the Act and its purpose would undoubtedly attract the provisions of Art. 19(5) care must always be taken in passing such acts that they provide sufficient safeguards against casual, capricious or even malicious exercise of the powers conferred by them. It is well known that the relevant provisions of the Act are initially put in motion against a person at a lower level than the District magistrate, and so it is always necessary that sufficient safeguards should be provided by the Act to protect the fundamental rights of innocent citizens and to save them from unnecessary harassment. That is why we think the definition of the word "goonda" should have given necessary assistance to the District Magistrate in deciding whether a particular citizen falls under the category of goonda or not; that is another infirmity in the Act. As we have already pointed out s. 4-A suffers from the same infirmities as s. 4.
>
> Having regard to the two infirmities in Sections 4, 4-A respectively we do not think it would be possible to accede to the argument of the Learned Advocate-General that the operative portion of the Act can fall under Art. 19(5) of the Constitution. The

> person against whom action can be taken under the Act is not entitled to know the source of the information received by the District Magistrate; he is only told about his prejudicial activities on which the satisfaction of the District Magistrate is based that action should be taken against him under s.4 or s. 4-A. In such a case it is absolutely essential that the Act must clearly indicate by a proper definition or otherwise when and under what circumstances a person can be called a goonda, and it must impose an obligation on the District Magistrate to apply his mind to the question as to whether the person against whom complaints are received is such a goonda or not. It has been urged before us that such an obligation is implicit in Sections 4 and 4-A. We are, however, not impressed by this argument. Where a statute empowers the specified authorities to take preventive action against the citizens it is essential that it should expressly make it a part of the duty of the said authorities to satisfy themselves about the existence of what the statute regards as conditions precedent to the exercise of the said authority. If the statute is silent in respect of one of such conditions precedent it undoubtedly constitutes a serious infirmity which would inevitably take it out of the provisions of Art. 19(5). The result of this infirmity is that it has left to the unguided and unfettered discretion of the authority concerned to treat any citizen as a goonda. In other words, the restrictions which it allows to be imposed on the exercise of the fundamental right of a citizen guaranteed by Art. 19(1)(d) and (e) must in the circumstances be held to be unreasonable. That is the view taken by the High court and we see no reason to differ from it." (at pages 979, 980)

65. At one time this Court seemed to suggest that the doctrine of vagueness was no part of the Constitutional Law of

India. That was dispelled in no uncertain terms in **K.A. Abbas v. The Union of India & Another,** [1971] 2 S.C.R. 446:

> "This brings us to the manner of the exercise of control and restriction by the directions. Here the argument is that most of the regulations are vague and further that they leave no scope for the exercise of creative genius in the field of art. This poses the first question before us whether the 'void for vagueness' doctrine is applicable. Reliance in this connection is placed on Municipal Committee Amritsar and Anr. v. The State of Rajasthan . In that case a Division Bench of this Court lays down that an Indian Act cannot be declared invalid on the ground that it violates the due process clause or that it is vague……" (at page 469)
>
> "These observations which are clearly obiter are apt to be too generally applied and need to be explained. While it is true that the principles evolved by the Supreme Court of the United States of America in the application of the Fourteenth Amendment were eschewed in our Constitution and instead the limits of restrictions on each fundamental right were indicated in the clauses that follow the first clause of the nineteenth article, it cannot be said as an absolute principle that no law will be considered bad for sheer vagueness. There is ample authority for the proposition that a law affecting fundamental rights may be so considered. A very pertinent example is to be found in State of Madhya Pradesh and Anr. v. Baldeo Prasad, 1961 (1) SCR 970 where the Central Provinces and Berar Goondas Act 1946 was declared void for uncertainty. The condition for the application of Sections 4 and 4A was that the person sought to be proceeded against must be a goonda but the definition of goonda in the Act indicated no tests for deciding which person fell within the definition. The

provisions were therefore held to be uncertain and vague.

The real rule is that if a law is vague or appears to be so, the court must try to construe it, as far as may be, and language permitting, the construction sought to be placed on it, must be in accordance with the intention of the legislature. Thus if the law is open to diverse construction, that construction which accords best with the intention of the legislature and advances the purpose of legislation, is to be preferred. Where however the law admits of no such construction and the persons applying it are in a boundless sea of uncertainty and the law prima facie takes away a guaranteed freedom, the law must be held to offend the Constitution as was done in the case of the Goonda Act. This is not application of the doctrine of due process. The invalidity arises from the probability of the misuse of the law to the detriment of the individual. If possible, the Court instead of striking down the law may itself draw the line of demarcation where possible but this effort should be sparingly made and only in the clearest of cases." (at pages 470, 471)

66. Similarly, in **Harakchand Ratanchand Banthia & Ors.** v. **Union of India & Ors.**, 1969 (2) SCC 166, Section 27 of the Gold Control Act was struck down on the ground that the conditions imposed by it for the grant of renewal of licences are uncertain, vague and unintelligible. The Court held:

"21. We now come to Section 27 of the Act which relates to licensing of dealers. It was stated on behalf of the petitioners that the conditions imposed by sub-section (6) of Section 27 for the grant or

renewal of licences are uncertain, vague and unintelligible and consequently wide and unfettered power was conferred upon the statutory authorities in the matter of grant or renewal of licence. In our opinion this contention is well founded and must be accepted as correct. Section 27(6)(*a*) states that in the matter of issue or renewal of licences the Administrator shall have regard to "the number of dealers existing in the region in which the applicant intends to carry on business as a dealer". But the word "region" is nowhere defined in the Act. Similarly Section 27(6)(*b*) requires the Administrator to have regard to "the anticipated demand, as estimated by him, for ornaments in that region." The expression "anticipated demand" is a vague expression which is not capable of objective assessment and is bound to lead to a great deal of uncertainty. Similarly the expression "suitability of the applicant" in Section 27(6)(*e*) and "public interest" in Section 27(6)(*g*) do not provide any objective standard or norm or guidance. For these reasons it must be held that clauses (*a*),(*d*),(*e*) and (*g*) of Section 27(6) impose unreasonable restrictions on the fundamental right of the petitioner to carry on business and are constitutionally invalid. It was also contended that there was no reason why the conditions for renewal of licence should be as rigorous as the conditions for initial grant of licence. The requirement of strict conditions for the renewal of licence renders the entire future of the business of the dealer uncertain and subjects it to the caprice and arbitrary will of the administrative authorities. There is justification for this argument and the requirement of Section 26 of the Act imposing the same conditions for the renewal of the licence as for the initial grant appears to be unreasonable. In our opinion clauses (*a*), (*b*), (*e*) and (*g*) are inextricably bound up with the other clauses of Section 27(6) and form part of a single scheme. The result is that clauses (*a*), (*b*), (*c*), (*e*) and (*g*) are not severable

> and the entire Section 27(6) of the Act must be held invalid. Section 27(2)(*d*) of the Act states that a valid licence issued by the Administrator "may contain such conditions, limitations and restrictions as the Administrator may think fit to impose and different conditions, limitations and restrictions may be imposed for different classes of dealers". On the face of it, this sub-section confers such wide and vague power upon the Administrator that it is difficult to limit its scope. In our opinion Section 27(2)(*d*) of the Act must be struck down as an unreasonable restriction on the fundamental right of the petitioners to carry on business. It appears, however, to us that if Section 27(2)(*d*) and Section 27(6) of the Act are invalid the licensing scheme contemplated by the rest of Section 27 of the Act cannot be worked in practice. It is, therefore, necessary for Parliament to enact fresh legislation imposing appropriate conditions and restrictions for the grant and renewal of licences to dealers. In the alternative the Central Government may make appropriate rules for the same purpose in exercise of its rule-making power under Section 114 of the Act."

67. In **A.K. Roy & Ors.** v. **Union of India & Ors.,** [1982] 2 S.C.R. 272, a part of Section 3 of the National Security Ordinance was read down on the ground that "acting in any manner prejudicial to the maintenance of supplies and services essential to the community" is an expression so vague that it is capable of wanton abuse. The Court held:

> "What we have said above in regard to the expressions 'defence of India', 'security of India',

'security of the State' and ‘relations of India with foreign powers’ cannot apply to the expression “acting in any manner prejudicial to the maintenance of supplies and services essential to the community” which occurs in Section 3(2) of the Act. Which supplies and services are essential to the community can easily be defined by the legislature and indeed, legislations which regulate the prices and possession of essential commodities either enumerate those commodities or confer upon the appropriate Government the power to do so. In the absence of a definition of ‘supplies and services essential to the community’, the detaining authority will be free to extend the application of this clause of sub-section (2) to any commodities or services the maintenance of supply of which, according to him, is essential to the community.

But that is not all. The Explanation to sub-section (2) gives to the particular phrase in that sub-section a meaning which is not only uncertain but which, at any given point of time, will be difficult to ascertain or fasten upon. According to the Explanation, no order of detention can be made under the National Security Act on any ground on which an order of detention may be made under the Prevention of Blackmarketing and Maintenance of Supplies of Essential Commodities Act, 1980. The reason for this, which is stated in the Explanation itself, is that for the purposes of sub-section (2), “acting in any manner prejudicial to the maintenance of supplies essential to the community” does not include “acting in any manner prejudicial to the maintenance of supplies of commodities essential to the community” as defined in the Explanation to sub-section (1) of Section 3 of the Act of 1980. Clauses (*a*) and (*b*) of the Explanation to Section 3(1) of the Act of 1980 exhaust almost the entire range of essential commodities. Clause (*a*) relates to committing or instigating any person to commit any offence

punishable under the Essential Commodities Act, 10 of 1955, or under any other law for the time being in force relating to the control of the production, supply or distribution of, or trade and commerce in, any commodity essential to the community. Clause (*b*) of the Explanation to Section 3(1) of the Act of 1980 relates to dealing in any commodity which is an essential commodity as defined in the Essential Commodities Act, 1955, or with respect to which provisions have been made in any such other law as is referred to in clause (*a*). We find it quite difficult to understand as to which are the remaining commodities outside the scope of the Act of 1980, in respect of which it can be said that the maintenance of their supplies is essential to the community. The particular clause in sub-section (2) of Section 3 of the National Security Act is, therefore, capable of wanton abuse in that, the detaining authority can place under detention any person for possession of any commodity on the basis that the authority is of the opinion that the maintenance of supply of that commodity is essential to the community. We consider the particular clause not only vague and uncertain but, in the context of the Explanation, capable of being extended cavalierly to supplies, the maintenance of which is not essential to the community. To allow the personal liberty of the people to be taken away by the application of that clause would be a flagrant violation of the fairness and justness of procedure which is implicit in the provisions of Article 21." (at page 325-326)

68. Similarly, in **Kartar Singh** v. **State of Punjab,** (1994) 3 SCC 569 at para 130-131, it was held:

"130. It is the basic principle of legal jurisprudence that an enactment is void for vagueness if its

> prohibitions are not clearly defined. Vague laws offend several important values. It is insisted or emphasized that laws should give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Such a law impermissibly delegates basic policy matters to policemen and also judges for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. More so uncertain and undefined words deployed inevitably lead citizens to "steer far wider of the unlawful zone … than if the boundaries of the forbidden areas were clearly marked.
>
> 131. Let us examine clause (*i*) of Section 2(1)(*a*). This section is shown to be blissfully and impermissibly vague and imprecise. As rightly pointed out by the learned counsel, even an innocent person who ingenuously and undefiledly communicates or associates without any knowledge or having no reason to believe or suspect that the person or class of persons with whom he has communicated or associated is engaged in assisting in any manner terrorists or disruptionists, can be arrested and prosecuted by abusing or misusing or misapplying this definition. In ultimate consummation of the proceedings, perhaps that guiltless and innoxious innocent person may also be convicted."

69. Judged by the standards laid down in the aforesaid judgments, it is quite clear that the expressions used in 66A are completely open-ended and undefined. Section 66 in stark contrast to Section 66A states:

> "66. **Computer related offences**.—If any person, dishonestly or fraudulently, does any act referred to in Section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
>
> *Explanation*.—For the purposes of this section,—
>
> (*a*) the word "dishonestly" shall have the meaning assigned to it in Section 24 of the Indian Penal Code (45 of 1860);
>
> (*b*) the word "fraudulently" shall have the meaning assigned to it in Section 25 of the Indian Penal Code (45 of 1860)."

70. It will be clear that in all computer related offences that are spoken of by Section 66, *mens rea* is an ingredient and the expression "dishonestly" and "fraudulently" are defined with some degree of specificity, unlike the expressions used in Section 66A.

71. The provisions contained in Sections 66B up to Section 67B also provide for various punishments for offences that are clearly made out. For example, under Section 66B, whoever dishonestly receives or retains any stolen computer resource or communication device is punished with imprisonment. Under

Section 66C, whoever fraudulently or dishonestly makes use of any identification feature of another person is liable to punishment with imprisonment. Under Section 66D, whoever cheats by personating becomes liable to punishment with imprisonment. Section 66F again is a narrowly drawn section which inflicts punishment which may extend to imprisonment for life for persons who threaten the unity, integrity, security or sovereignty of India. Sections 67 to 67B deal with punishment for offences for publishing or transmitting obscene material including depicting children in sexually explicit acts in electronic form.

72. In the Indian Penal Code, a number of the expressions that occur in Section 66A occur in Section 268.

> "268. **Public nuisance.**—A person is guilty of a public nuisance who does any act or is guilty of an illegal omission, which causes any common injury, danger or annoyance to the public or to the people in general who dwell or occupy property in the vicinity, or which must necessarily cause injury, obstruction, danger or annoyance to persons who may have occasion to use any public right.

> A common nuisance is not excused on the ground that it causes some convenience or advantage."

73. It is important to notice the distinction between the Sections 268 and 66A. Whereas, in Section 268 the various expressions used are ingredients for the offence of a public nuisance, these ingredients now become offences in themselves when it comes to Section 66A. Further, under Section 268, the person should be guilty of an act or omission which is illegal in nature – legal acts are not within its net. A further ingredient is that injury, danger or annoyance must be to the public in general. Injury, danger or annoyance are not offences by themselves howsoever made and to whomsoever made. The expression "annoyance" appears also in Sections 294 and 510 of the IPC:

> "294. **Obscene acts and songs.**—Whoever, to the annoyance of others,
>
> (*a*) does any obscene act in any public place, or
>
> (*b*) sings, recites or utters any obscene songs, ballad or words, in or near any public place,

> shall be punished with imprisonment of either description for a term which may extend to three months, or with fine, or with both.
>
> 510. **Misconduct in public by a drunken person.** —Whoever, in a state of intoxication, appears in any public place, or in any place which it is a trespass in him to enter, and there conducts himself in such a manner as to cause annoyance to any person, shall be punished with simple imprisonment for a term which may extend to twenty-four hours, or with fine which may extend to ten rupees, or with both."

74. If one looks at Section 294, the annoyance that is spoken of is clearly defined - that is, it has to be caused by obscene utterances or acts. Equally, under Section 510, the annoyance that is caused to a person must only be by another person who is in a state of intoxication and who annoys such person only in a public place or in a place for which it is a trespass for him to enter. Such narrowly and closely defined contours of offences made out under the Penal Code are conspicuous by their absence in Section 66A which in stark contrast uses completely open ended, undefined and vague language.

75. Incidentally, none of the expressions used in Section 66A are defined. Even "criminal intimidation" is not defined – and

the definition clause of the Information Technology Act, Section 2 does not say that words and expressions that are defined in the Penal Code will apply to this Act.

76. Quite apart from this, as has been pointed out above, every expression used is nebulous in meaning. What may be offensive to one may not be offensive to another. What may cause annoyance or inconvenience to one may not cause annoyance or inconvenience to another. Even the expression "persistently" is completely imprecise – suppose a message is sent thrice, can it be said that it was sent "persistently"? Does a message have to be sent (say) at least eight times, before it can be said that such message is "persistently" sent? There is no demarcating line conveyed by any of these expressions – and that is what renders the Section unconstitutionally vague.

77. However, the learned Additional Solicitor General argued before us that expressions that are used in Section 66A may be incapable of any precise definition but for that reason they are not constitutionally vulnerable. He cited a large number of

judgments in support of this submission. None of the cited judgments dealt with a Section creating an offence which is saved despite its being vague and in capable of any precise definition. In fact, most of the judgments cited before us did not deal with criminal law at all. The few that did are dealt with hereinbelow. For instance, **Madan Singh** v. **State of Bihar**, (2004) 4 SCC 622 was cited before us. The passage cited from the aforesaid judgment is contained in para 19 of the judgment. The cited passage is not in the context of an argument that the word "terrorism" not being separately defined would, therefore, be struck down on the ground of vagueness. The cited passage was only in the context of upholding the conviction of the accused in that case. Similarly, in **Zameer Ahmed Latifur Rehman Sheikh** v. **State of Maharashtra & Ors.,** (2010) 5 SCC 246, the expression "insurgency" was said to be undefined and would defy a precise definition, yet it could be understood to mean break down of peace and tranquility as also a grave disturbance of public order so as to endanger the security of the State and its sovereignty. This again was said in the context of a challenge on the ground of legislative competence. The

provisions of the Maharashtra Control of Organised Crime Act were challenged on the ground that they were outside the expression "public order" contained in Entry 1 of List I of the 7th Schedule of the Constitution of India. This contention was repelled by saying that the expression "public order" was wide enough to encompass cases of "insurgency". This case again had nothing to do with a challenge raised on the ground of vagueness.

78. Similarly, in **State of M.P.** v. **Kedia Leather & Liquor Limited,** (2003) 7 SCC 389, paragraph 8 was cited to show that the expression "nuisance" appearing in Section 133 of the Code of Criminal Procedure was also not capable of precise definition. This again was said in the context of an argument that Section 133 of the Code of Criminal Procedure was impliedly repealed by the Water (Prevention and Control of Pollution) Act, 1974. This contention was repelled by saying that the areas of operation of the two provisions were completely different and they existed side by side being mutually exclusive. This case again did not contain any

argument that the provision contained in Section 133 was vague and, therefore, unconstitutional. Similarly, in **State of Karnataka** v. **Appa Balu Ingale,** 1995 Supp. (4) SCC 469, the word "untouchability" was said not to be capable of precise definition. Here again, there was no constitutional challenge on the ground of vagueness.

79. In fact, two English judgments cited by the learned Additional Solicitor General would demonstrate how vague the words used in Section 66A are. In **Director of Public Prosecutions** v. **Collins**, (2006) 1 WLR 2223, the very expression "grossly offensive" is contained in Section 127(1)(1) of the U.K. Communications Act, 2003. A 61 year old man made a number of telephone calls over two years to the office of a Member of Parliament. In these telephone calls and recorded messages Mr. Collins who held strong views on immigration made a reference to "Wogs", "Pakis", "Black bastards" and "Niggers". Mr. Collins was charged with sending messages which were grossly offensive. The Leicestershire Justices dismissed the case against Mr. Collins on the ground that the telephone calls were offensive but not grossly

offensive. A reasonable person would not so find the calls to be grossly offensive. The Queen's Bench agreed and dismissed the appeal filed by the Director of Public Prosecutions. The House of Lords reversed the Queen's Bench stating:

> "9. The parties agreed with the rulings of the Divisional Court that it is for the Justices to determine as a question of fact whether a message is grossly offensive, that in making this determination the Justices must apply the standards of an open and just multi-racial society, and that the words must be judged taking account of their context and all relevant circumstances. I would agree also. Usages and sensitivities may change over time. Language otherwise insulting may be used in an unpejorative, even affectionate, way, or may be adopted as a badge of honour ("Old Contemptibles"). There can be no yardstick of gross offensiveness otherwise than by the application of reasonably enlightened, but not perfectionist, contemporary standards to the particular message sent in its particular context. The test is whether a message is couched in terms liable to cause gross offence to those to whom it relates.
>
> 10. In contrast with section 127(2)(a) and its predecessor subsections, which require proof of an unlawful purpose and a degree of knowledge, section 127(1)(a) provides no explicit guidance on the state of mind which must be proved against a defendant to establish an offence against the subsection."

80. Similarly in **Chambers** v. **Director of Public Prosecutions**, [2013] 1 W.L.R. 1833, the Queen's Bench was faced with the following facts:

> "Following an alert on the Internet social network, Twitter, the defendant became aware that, due to adverse weather conditions, an airport from which he was due to travel nine days later was closed. He responded by posting several "tweets" on Twitter in his own name, including the following: "Crap1 Robin Hood Airport is closed. You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high1" None of the defendant's "followers" who read the posting was alarmed by it at the time. Some five days after its posting the defendant's tweet was read by the duty manager responsible for security at the airport on a general Internet search for tweets relating to the airport. Though not believed to be a credible threat the matter was reported to the police. In interview the defendant asserted that the tweet was a joke and not intended to be menacing. The defendant was charged with sending by a public electronic communications network a message of a menacing character contrary to section 127(1)(a) of the Communications Act 2003. He was convicted in a magistrates' court and, on appeal, the Crown Court upheld the conviction, being satisfied that the message was "menacing per se" and that the defendant was, at the very least, aware that his message was of a menacing character."

81. The Crown Court was satisfied that the message in question was "menacing" stating that an ordinary person seeing

the tweet would be alarmed and, therefore, such message would be "menacing". The Queen's Bench Division reversed the Crown Court stating:

> "31. Before concluding that a message is criminal on the basis that it represents a menace, its precise terms, and any inferences to be drawn from its precise terms, need to be examined in the context in and the means by which the message was sent. The Crown Court was understandably concerned that this message was sent at a time when, as we all know, there is public concern about acts of terrorism and the continuing threat to the security of the country from possible further terrorist attacks. That is plainly relevant to context, but the offence is not directed to the inconvenience which may be caused by the message. In any event, the more one reflects on it, the clearer it becomes that this message did not represent a terrorist threat, or indeed any other form of threat. It was posted on "Twitter" for widespread reading, a conversation piece for the defendant's followers, drawing attention to himself and his predicament. Much more significantly, although it purports to address "you", meaning those responsible for the airport, it was not sent to anyone at the airport or anyone responsible for airport security, or indeed any form of public security. The grievance addressed by the message is that the airport is closed when the writer wants it to be open. The language and punctuation are inconsistent with the writer intending it to be or it to be taken as a serious warning. Moreover, as Mr. Armson noted, it is unusual for a threat of a terrorist nature to invite the person making it to be readily identified, as this message did. Finally, although we are accustomed to very brief messages by terrorists to indicate that a bomb or explosive device has

> been put in place and will detonate shortly, it is difficult to imagine a serious threat in which warning of it is given to a large number of tweet "followers" in ample time for the threat to be reported and extinguished."

82. These two cases illustrate how judicially trained minds would find a person guilty or not guilty depending upon the Judge's notion of what is "grossly offensive" or "menacing". In Collins' case, both the Leicestershire Justices and two Judges of the Queen's Bench would have acquitted Collins whereas the House of Lords convicted him. Similarly, in the Chambers case, the Crown Court would have convicted Chambers whereas the Queen's Bench acquitted him. If judicially trained minds can come to diametrically opposite conclusions on the same set of facts it is obvious that expressions such as "grossly offensive" or "menacing" are so vague that there is no manageable standard by which a person can be said to have committed an offence or not to have committed an offence. Quite obviously, a prospective offender of Section 66A and the authorities who are to enforce Section 66A have absolutely no manageable standard by which to book a person for an offence under Section 66A. This being the case, having regard also to the two

English precedents cited by the learned Additional Solicitor General, it is clear that Section 66A is unconstitutionally vague.

Ultimately, applying the tests referred to in **Chintaman Rao** and **V.G. Row's** case, referred to earlier in the judgment, it is clear that Section 66A arbitrarily, excessively and disproportionately invades the right of free speech and upsets the balance between such right and the reasonable restrictions that may be imposed on such right.

Chilling Effect And Overbreadth

83. Information that may be grossly offensive or which causes annoyance or inconvenience are undefined terms which take into the net a very large amount of protected and innocent speech. A person may discuss or even advocate by means of writing disseminated over the internet information that may be a view or point of view pertaining to governmental, literary, scientific or other matters which may be unpalatable to certain sections of society. It is obvious that an expression of a view on any matter may cause annoyance, inconvenience or may be grossly offensive to some. A few examples will suffice. A

certain section of a particular community may be grossly offended or annoyed by communications over the internet by "liberal views" – such as the emancipation of women or the abolition of the caste system or whether certain members of a non proselytizing religion should be allowed to bring persons within their fold who are otherwise outside the fold. Each one of these things may be grossly offensive, annoying, inconvenient, insulting or injurious to large sections of particular communities and would fall within the net cast by Section 66A. In point of fact, Section 66A is cast so widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting with the mores of the day would be caught within its net. Such is the reach of the Section and if it is to withstand the test of constitutionality, the chilling effect on free speech would be total.

84. Incidentally, some of our judgments have recognized this chilling effect of free speech. In **R. Rajagopal v. State of T.N.**, (1994) 6 SCC 632, this Court held:

"19. The principle of *Sullivan* [376 US 254 : 11 L Ed 2d 686 (1964)] was carried forward — and this is relevant to the second question arising in this case — in *Derbyshire County Council* v. *Times Newspapers Ltd.* [(1993) 2 WLR 449 : (1993) 1 All ER 1011, HL] , a decision rendered by the House of Lords. The plaintiff, a local authority brought an action for damages for libel against the defendants in respect of two articles published in *Sunday Times* questioning the propriety of investments made for its superannuation fund. The articles were headed "*Revealed: Socialist tycoon deals with Labour Chief*" and "*Bizarre deals of a council leader and the media tycoon*". A preliminary issue was raised whether the plaintiff has a cause of action against the defendant. The trial Judge held that such an action was maintainable but on appeal the Court of Appeal held to the contrary. When the matter reached the House of Lords, it affirmed the decision of the Court of Appeal but on a different ground. Lord Keith delivered the judgment agreed to by all other learned Law Lords. In his opinion, Lord Keith recalled that in *Attorney General* v. *Guardian Newspapers Ltd. (No. 2)*[(1990) 1 AC 109 : (1988) 3 All ER 545 : (1988) 3 WLR 776, HL] popularly known as "*Spycatcher case*", the House of Lords had opined that "there are rights available to private citizens which institutions of… Government are not in a position to exercise unless they can show that it is in the public interest to do so". It was also held therein that not only was there no public interest in allowing governmental institutions to sue for libel, it was "contrary to the public interest because to admit such actions would place an undesirable fetter on freedom of speech" and further that action for defamation or threat of such action "inevitably have an inhibiting effect on freedom of speech". The learned Law Lord referred to the decision of the United States Supreme Court in *New York Times* v. *Sullivan* [376 US 254 : 11 L Ed 2d 686

> (1964)] and certain other decisions of American Courts and observed — and this is significant for our purposes—
>
> "while these decisions were related most directly to the provisions of the American Constitution concerned with securing freedom of speech, *the public interest considerations which underlaid them are no less valid in this country. What has been described as 'the chilling effect'* induced by the threat of civil actions for libel is very important. Quite often the facts which would justify a defamatory publication are known to be true, but admissible evidence capable of proving those facts is not available."
>
> Accordingly, it was held that the action was not maintainable in law."

85. Also in **S. Khushboo v. Kanniammal**, (2010) 5 SCC 600, this Court said:

> "47. In the present case, the substance of the controversy does not really touch on whether premarital sex is socially acceptable. Instead, the real issue of concern is the disproportionate response to the appellant's remarks. If the complainants vehemently disagreed with the appellant's views, then they should have contested her views through the news media or any other public platform. The law should not be used in a manner that has chilling effects on the "freedom of speech and expression".

86. That the content of the right under Article 19(1)(a) remains the same whatever the means of communication including internet communication is clearly established by

Reno's case (supra) and by **The Secretary, Ministry of Information & Broadcasting** v. **Cricket Association of Bengal & Anr.,** (1995) SCC 2 161 at Para 78 already referred to. It is thus clear that not only are the expressions used in Section 66A expressions of inexactitude but they are also over broad and would fall foul of the repeated injunctions of this Court that restrictions on the freedom of speech must be couched in the narrowest possible terms. For example, see, **Kedar Nath Singh** v. **State of Bihar,** [1962] Supp. 2 S.C.R. 769 at 808 -809. In point of fact, judgments of the Constitution Bench of this Court have struck down sections which are similar in nature. A prime example is the section struck down in the first **Ram Manohar Lohia case**, namely, Section 3 of the U.P. Special Powers Act, where the persons who "instigated" expressly or by implication any person or class of persons not to pay or to defer payment of any liability were punishable. This Court specifically held that under the Section a wide net was cast to catch a variety of acts of instigation ranging from friendly advice to systematic propaganda. It was held that in its wide amplitude, the Section takes in the innocent as well as the

guilty, bonafide and malafide advice and whether the person be a legal adviser, a friend or a well wisher of the person instigated, he cannot escape the tentacles of the Section. The Court held that it was not possible to predicate with some kind of precision the different categories of instigation falling within or without the field of constitutional prohibitions. It further held that the Section must be declared unconstitutional as the offence made out would depend upon factors which are uncertain.

87. In **Kameshwar Prasad & Ors.** v. **The State of Bihar & Anr.**, [1962] Supp. 3 S.C.R. 369, Rule 4-A of the Bihar Government Servants Conduct Rules, 1956 was challenged. The rule states "No government servant shall participate in any demonstration or resort to any form of strike in connection with any matter pertaining to his conditions of service."

88. The aforesaid rule was challenged under Articles 19 (1)(a) and (b) of the Constitution. The Court followed the law laid down in **Ram Manohar Lohia's** case [1960] 2 S.C.R. 821 and

accepted the challenge. It first held that demonstrations are a form of speech and then held:

> "The approach to the question regarding the constitutionality of the rule should be whether the ban that it imposes on demonstrations would be covered by the limitation of the guaranteed rights contained in Art. 19 (2) and 19(3). In regard to both these clauses the only relevant criteria which has been suggested by the respondent-State is that the rule is framed "in the interest of public order". A demonstration may be defined as "an expression of one's feelings by outward signs." A demonstration such as is prohibited by, the rule may be of the most innocent type - peaceful orderly such as the mere wearing of a badge by a Government servant or even by a silent assembly say outside office hours - demonstrations which could in no sense be suggested to involve any breach of tranquility, or of a type involving incitement to or capable of leading to disorder. If the rule had confined itself to demonstrations of type which would lead to disorder then the validity of that rule could have been sustained but what the rule does is the imposition of a blanket-ban on all demonstrations of whatever type - innocent as well as otherwise - and in consequence its validity cannot be upheld." (at page 374)

89. The Court further went on to hold that remote disturbances of public order by demonstration would fall outside Article 19(2). The connection with public order has to be intimate, real and rational and should arise directly from the

demonstration that is sought to be prohibited. Finally, the Court held:

> "The vice of the rule, in our opinion, consists in this that it lays a ban on every type of demonstration - be the same however innocent and however incapable of causing a breach of public tranquility and does not confine itself to those forms of demonstrations which might lead to that result." (at page 384)

90. These two Constitution Bench decisions bind us and would apply directly on Section 66A. We, therefore, hold that the Section is unconstitutional also on the ground that it takes within its sweep protected speech and speech that is innocent in nature and is liable therefore to be used in such a way as to have a chilling effect on free speech and would, therefore, have to be struck down on the ground of overbreadth.

Possibility of an act being abused is not a ground to test its validity:

91. The learned Additional Solicitor General cited a large number of judgments on the proposition that the fact that Section 66A is capable of being abused by the persons who administered it is not a ground to test its validity if it is otherwise valid. He further assured us that this Government was

committed to free speech and that Section 66A would not be used to curb free speech, but would be used only when excesses are perpetrated by persons on the rights of others. In **The Collector of Customs, Madras v. Nathella Sampathu Chetty & Anr.,** [1962] 3 S.C.R. 786, this Court observed:

> "….This Court has held in numerous rulings, to which it is unnecessary to refer, that the possibility of the abuse of the powers under the provisions contained in any statute is no ground for declaring the provision to be unreasonable or void. Commenting on a passage in the judgment of the Court of Appeal of Northern Ireland which stated:
>
> "If such powers are capable of being exercised reasonably it is impossible to say that they may not also be exercised unreasonably"
>
> and treating this as a ground for holding the statute invalid Viscount Simonds observed in *Belfast Corporation* v. *O.D. Commission* [1960 AC 490 at pp. 520-521] :
>
> "It appears to me that the short answer to this contention (and I hope its shortness will not be regarded as disrespect) is that the validity of a measure is not to be determined by its application to particular cases…. If it is not so exercised (i.e. if the powers are abused) it is open to challenge and there is no need for express provision for its challenge in the statute."
>
> The possibility of abuse of a statute otherwise valid does not impart to it any element of invalidity. The converse must also follow that a statute which is

> otherwise invalid as being unreasonable cannot be saved by its being administered in a reasonable manner. The constitutional validity of the statute would have to be determined on the basis of its provisions and on the ambit of its operation as reasonably construed. If so judged it passes the test of reasonableness, possibility of the powers conferred being improperly used is no ground for pronouncing the law itself invalid and similarly if the law properly interpreted and tested in the light of the requirements set out in Part III of the Constitution does not pass the test it cannot be pronounced valid merely because it is administered in a manner which might not conflict with the constitutional requirements." (at page 825)

92. In this case, it is the converse proposition which would really apply if the learned Additional Solicitor General's argument is to be accepted. If Section 66A is otherwise invalid, it cannot be saved by an assurance from the learned Additional Solicitor General that it will be administered in a reasonable manner. Governments may come and Governments may go but Section 66A goes on forever. An assurance from the present Government even if carried out faithfully would not bind any successor Government. It must, therefore, be held that Section 66A must be judged on its own merits without any reference to how well it may be administered.

Severability:

93. The argument of the learned Additional Solicitor General on this score is reproduced by us verbatim from one of his written submissions:

> "Furthermore it is respectfully submitted that in the event of Hon'ble Court not being satisfied about the constitutional validity of either any expression or a part of the provision, the Doctrine of Severability as enshrined under Article 13 may be resorted to."

94. The submission is vague: the learned Additional Solicitor General does not indicate which part or parts of Section 66A can possibly be saved. This Court in **Romesh Thappar v. The State of Madras,** [1950] S.C.R. 594 repelled a contention of severability when it came to the courts enforcing the fundamental right under Article 19(1)(a) in the following terms:

> "It was, however, argued that Section 9(1-A) could not be considered wholly void, as, under Article 13(1), an existing law inconsistent with a fundamental right is void only to the extent of the inconsistency and no more. Insofar as the securing of the public safety or the maintenance of public order would include the security of the State, the impugned provision, as applied to the latter purpose, was covered by clause (2) of Article 19

> and must, it was said, be held to be valid. We are unable to accede to this contention. Where a law purports to authorise the imposition of restrictions on a fundamental right in language wide enough to cover restrictions both within and without the limits of constitutionally permissible legislative action affecting such right, it is not possible to uphold it even so far as it may be applied within the constitutional limits, as it is not severable. So long as the possibility of its being applied for purposes not sanctioned by the Constitution cannot be ruled out, it must be held to be wholly unconstitutional and void. In other words, clause (2) of Article 19 having allowed the imposition of restrictions on the freedom of speech and expression only in cases where danger to the State is involved, an enactment, which is capable of being applied to cases where no such danger could arise, cannot be held to be constitutional and valid to any extent." (At page 603)

95. It has been held by us that Section 66A purports to authorize the imposition of restrictions on the fundamental right contained in Article 19(1)(a) in language wide enough to cover restrictions both within and without the limits of constitutionally permissible legislative action. We have held following K.A. Abbas' case (Supra) that the possibility of Section 66A being applied for purposes not sanctioned by the Constitution cannot be ruled out. It must, therefore, be held to be wholly unconstitutional and void. **Romesh Thappar's** Case was

distinguished in **R.M.D. Chamarbaugwalla v. The Union of India,** [1957] S.C.R. 930 in the context of a right under Article 19(1)(g) as follows:

> "20. In *Romesh Thappar* v. *State of Madras* [(1950) SCR 594] , the question was as to the validity of Section 9(1-A) of the Madras Maintenance of Public Order Act, 23 of 1949. That section authorised the Provincial Government to prohibit the entry and circulation within the State of a newspaper "for the purpose of securing the public safety or the maintenance of public order." Subsequent to the enactment of this statute, the Constitution came into force, and the validity of the impugned provision depended on whether it was protected by Article 19(2), which saved "existing law insofar as it relates to any matter which undermines the security of or tends to overthrow the State." It was held by this Court that as the purposes mentioned in Section 9(1-A) of the Madras Act were wider in amplitude than those specified in Article 19(2), and as it was not possible to split up Section 9(1-A) into what was within and what was without the protection of Article 19(2), the provision must fail in its entirety. That is really a decision that the impugned provision was on its own contents inseverable. It is not an authority for the position that even when a provision is severable, it must be struck down on the ground that the principle of severability is inadmissible when the invalidity of a statute arises by reason of its contravening constitutional prohibitions. It should be mentioned that the decision in *Romesh Thappar* v. *State of Madras* [(1950) SCR 594] was referred to in *State of Bombay* v. *F.N. Balsara* [(1951) SCR 682] and *State of*

Bombay v. *United Motors* (*India*) *Ltd.* [(1953) SCR 1069 at 1098-99] and distinguished."

96. The present being a case of an Article 19(1)(a) violation, **Romesh Thappar's** judgment would apply on all fours. In an Article 19(1)(g) challenge, there is no question of a law being applied for purposes not sanctioned by the Constitution for the simple reason that the eight subject matters of Article 19(2) are conspicuous by their absence in Article 19(6) which only speaks of reasonable restrictions in the interests of the general public. The present is a case where, as has been held above, Section 66A does not fall within any of the subject matters contained in Article 19(2) and the possibility of its being applied for purposes outside those subject matters is clear. We therefore hold that no part of Section 66A is severable and the provision as a whole must be declared unconstitutional.

Article 14

97. Counsel for the petitioners have argued that Article 14 is also infringed in that an offence whose ingredients are vague in nature is arbitrary and unreasonable and would result in

arbitrary and discriminatory application of the criminal law. Further, there is no intelligible differentia between the medium of print, broadcast, and real live speech as opposed to speech on the internet and, therefore, new categories of criminal offences cannot be made on this ground. Similar offences which are committed on the internet have a three year maximum sentence under Section 66A as opposed to defamation which has a two year maximum sentence. Also, defamation is a non-cognizable offence whereas under Section 66A the offence is cognizable.

98. We have already held that Section 66A creates an offence which is vague and overbroad, and, therefore, unconstitutional under Article 19(1)(a) and not saved by Article 19(2). We have also held that the wider range of circulation over the internet cannot restrict the content of the right under Article 19(1)(a) nor can it justify its denial. However, when we come to discrimination under Article 14, we are unable to agree with counsel for the petitioners that there is no intelligible differentia between the medium of print, broadcast and real live speech as

opposed to speech on the internet. The intelligible differentia is clear – the internet gives any individual a platform which requires very little or no payment through which to air his views. The learned Additional Solicitor General has correctly said that something posted on a site or website travels like lightning and can reach millions of persons all over the world. If the petitioners were right, this Article 14 argument would apply equally to all other offences created by the Information Technology Act which are not the subject matter of challenge in these petitions. We make it clear that there is an intelligible differentia between speech on the internet and other mediums of communication for which separate offences can certainly be created by legislation. We find, therefore, that the challenge on the ground of Article 14 must fail.

Procedural Unreasonableness

99. One other argument must now be considered. According to the petitioners, Section 66A also suffers from the vice of procedural unreasonableness. In that, if, for example, criminal defamation is alleged, the safeguards available under Section

199 Cr.P.C. would not be available for a like offence committed under Section 66A. Such safeguards are that no court shall take cognizance of such an offence except upon a complaint made by some person aggrieved by the offence and that such complaint will have to be made within six months from the date on which the offence is alleged to have been committed. Further, safeguards that are to be found in Sections 95 and 96 of the Cr.P.C. are also absent when it comes to Section 66A. For example, where any newspaper book or document wherever printed appears to contain matter which is obscene, hurts the religious feelings of some community, is seditious in nature, causes enmity or hatred to a certain section of the public, or is against national integration, such book, newspaper or document may be seized but under Section 96 any person having any interest in such newspaper, book or document may within two months from the date of a publication seizing such documents, books or newspapers apply to the High court to set aside such declaration. Such matter is to be heard by a Bench consisting of at least three Judges or in High Courts which

consist of less than three Judges, such special Bench as may be composed of all the Judges of that High Court.

100. It is clear that Sections 95 and 96 of the Criminal Procedure Code reveal a certain degree of sensitivity to the fundamental right to free speech and expression. If matter is to be seized on specific grounds which are relatable to the subject matters contained in Article 19(2), it would be open for persons affected by such seizure to get a declaration from a High Court consisting of at least three Judges that in fact publication of the so-called offensive matter does not in fact relate to any of the specified subjects contained in Article 19(2).

Further, Section 196 of the Cr.P.C. states:

> "196. **Prosecution for offences against the State and for criminal conspiracy to commit such offence.**— (1) No Court shall take cognizance of—
>
> (*a*) any offence punishable under Chapter VI or under Section 153-A, [Section 295-A or sub-section (1) of Section 505] of the Indian Penal Code, 1860 (45 of 1860), or
>
> (*b*) a criminal conspiracy to commit such offence, or
>
> (*c*) any such abetment, as is described in Section 108-A of the Indian Penal Code (45 of 1860),

except with the previous sanction of the Central Government or of the State Government.

[(1-A)

No Court shall take cognizance of—

(*a*) any offence punishable under Section 153-B or sub-section (2) or sub-section (3) of Section 505 of the Indian Penal Code, 1860 (45 of 1860), or

(*b*) a criminal conspiracy to commit such offence,

except with the previous sanction of the Central Government or of the State Government or of the District Magistrate.]

(2) No court shall take cognizance of the offence of any criminal conspiracy punishable under Section 120-B of the Indian Penal Code (45 of 1860), other than a criminal conspiracy to commit [an offence] punishable with death, imprisonment for life or rigorous imprisonment for a term of two years or upwards, unless the State Government or the District Magistrate has consented in writing to the initiation of the proceedings:

Provided that where the criminal conspiracy is one to which the provisions of Section 195 apply, no such consent shall be necessary.

(3) The Central Government or the State Government may, before according sanction [under sub-section (1) or sub-section (1-A) and the District Magistrate may, before according sanction under sub-section (1-A)] and the State Government or the District Magistrate may, before giving consent under sub-section (2), order a preliminary investigation by a police officer not being below the rank of Inspector, in which case such police officer shall have the powers referred to in sub-section (3) of Section 155."

101. Again, for offences in the nature of promoting enmity between different groups on grounds of religion etc. or offences relatable to deliberate and malicious acts intending to outrage religious feelings or statements that create or promote enmity, hatred or ill-will between classes can only be taken cognizance of by courts with the previous sanction of the Central Government or the State Government. This procedural safeguard does not apply even when a similar offence may be committed over the internet where a person is booked under Section 66A instead of the aforesaid Sections.

Having struck down Section 66A on substantive grounds, we need not decide the procedural unreasonableness aspect of the Section.

Section 118 of the Kerala Police Act.

102. Learned counsel for the Petitioner in Writ Petition No. 196 of 2014 assailed sub-section (d) of Section 118 which is set out hereinbelow:

> "118. Penalty for causing grave violation of public order or danger.- Any person who,-

(d) Causes annoyance to any person in an indecent manner by statements or verbal or comments or telephone calls or calls of any type or by chasing or sending messages or mails by any means;
shall, on conviction be punishable with imprisonment for a term which may extend to three years or with fine not exceeding ten thousand rupees or with both."

103. Learned counsel first assailed the Section on the ground of legislative competence stating that this being a Kerala Act, it would fall outside Entries1 and 2 of List II and fall within Entry 31 of List I. In order to appreciate the argument we set out the relevant entries:

"List - I

31. Posts and telegraphs; telephones, wireless, broadcasting and other like forms of communication.

List - II

1. Public order (but not including the use of any naval, military or air force or any other armed force of the Union or of any other force subject to the control of the Union or of any contingent or unit thereof in aid of the civil power).

2. Police (including railway and village police) subject to the provisions of entry 2A of List I."

The Kerala Police Act as a whole would necessarily fall under Entry 2 of List II. In addition, Section 118 would also fall within Entry 1 of List II in that as its marginal note tells us it deals with penalties for causing grave violation of public order or danger.

104. It is well settled that a statute cannot be dissected and then examined as to under what field of legislation each part would separately fall. In **A.S. Krishna** v. **State of Madras**, [1957] S.C.R. 399, the law is stated thus:

> "The position, then, might thus be summed up : When a law is impugned on the ground that it is ultra vires the powers of the legislature which enacted it, what has to be ascertained is the true character of the legislation. To do that, one must have regard to the enactment as a whole, to its objects and to the scope and effect of its provisions. If on such examination it is found that the legislation is in substance one on a matter assigned to the legislature, then it must be held to be valid in its entirety, even though it might incidentally trench on matters which are beyond its competence. It would be quite an erroneous approach to the question to view such a statute not as an organic whole, but as a mere collection of sections, then disintegrate it into parts, examine under what heads of legislation those parts would severally fall, and by that process determine what portions thereof are intra vires, and what are not." (at page 410)

105. It is, therefore, clear that the Kerala Police Act as a whole and Section 118 as part thereof falls in pith and substance within Entry 2 List II, notwithstanding any incidental encroachment that it may have made on any other Entry in List I. Even otherwise, the penalty created for causing annoyance in an indecent manner in pith and substance would fall within Entry 1 List III which speaks of criminal law and would thus be within the competence of the State Legislature in any case.

106. However, what has been said about Section 66A would apply directly to Section 118(d) of the Kerala Police Act, as causing annoyance in an indecent manner suffers from the same type of vagueness and over breadth, that led to the invalidity of Section 66A, and for the reasons given for striking down Section 66A, Section 118(d) also violates Article 19(1)(a) and not being a reasonable restriction on the said right and not being saved under any of the subject matters contained in Article 19(2) is hereby declared to be unconstitutional.

Section 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

107. Section 69A of the Information Technology Act has already been set out in paragraph 2 of the judgment. Under sub-section (2) thereof, the 2009 Rules have been framed. Under Rule 3, the Central Government shall designate by notification in the official gazette an officer of the Central Government not below the rank of a Joint Secretary as the Designated Officer for the purpose of issuing direction for blocking for access by the public any information referable to Section 69A of the Act. Under Rule 4, every organization as defined under Rule 2(g), (which refers to the Government of India, State Governments, Union Territories and agencies of the Central Government as may be notified in the Official Gazette by the Central Government)– is to designate one of its officers as the "Nodal Officer". Under Rule 6, any person may send their complaint to the "Nodal Officer" of the concerned Organization for blocking, which complaint will then have to be examined by the concerned Organization regard being had to the parameters laid down in Section 69A(1) and after being so

satisfied, shall transmit such complaint through its Nodal Officer to the Designated Officer in a format specified by the Rules. The Designated Officer is not to entertain any complaint or request for blocking directly from any person. Under Rule 5, the Designated Officer may on receiving any such request or complaint from the Nodal Officer of an Organization or from a competent court, by order direct any intermediary or agency of the Government to block any information or part thereof for the reasons specified in 69A(1). Under Rule 7 thereof, the request/complaint shall then be examined by a Committee of Government Personnel who under Rule 8 are first to make all reasonable efforts to identify the originator or intermediary who has hosted the information. If so identified, a notice shall issue to appear and submit their reply at a specified date and time which shall not be less than 48 hours from the date and time of receipt of notice by such person or intermediary. The Committee then examines the request and is to consider whether the request is covered by 69A(1) and is then to give a specific recommendation in writing to the Nodal Officer of the concerned Organization. It is only thereafter that the

Designated Officer is to submit the Committee's recommendation to the Secretary, Department of Information Technology who is to approve such requests or complaints. Upon such approval, the Designated Officer shall then direct any agency of Government or intermediary to block the offending information. Rule 9 provides for blocking of information in cases of emergency where delay caused would be fatal in which case the blocking may take place without any opportunity of hearing. The Designated Officer shall then, not later than 48 hours of the issue of the interim direction, bring the request before the Committee referred to earlier, and only on the recommendation of the Committee, is the Secretary Department of Information Technology to pass the final order. Under Rule 10, in the case of an order of a competent court in India, the Designated Officer shall, on receipt of a certified copy of a court order, submit it to the Secretary, Department of Information Technology and then initiate action as directed by the Court. In addition to the above safeguards, under Rule 14 a Review Committee shall meet at least once in two months and record its findings as to whether directions issued are in

accordance with Section 69A(1) and if it is of the contrary opinion, the Review Committee may set aside such directions and issue orders to unblock the said information. Under Rule 16, strict confidentiality shall be maintained regarding all the requests and complaints received and actions taken thereof.

108. Learned counsel for the petitioners assailed the constitutional validity of Section 69A, and assailed the validity of the 2009 Rules. According to learned counsel, there is no pre-decisional hearing afforded by the Rules particularly to the "originator" of information, which is defined under Section 2(za) of the Act to mean a person who sends, generates, stores or transmits any electronic message; or causes any electronic message to be sent, generated, stored or transmitted to any other person. Further, procedural safeguards such as which are provided under Section 95 and 96 of the Code of Criminal Procedure are not available here. Also, the confidentiality provision was assailed stating that it affects the fundamental rights of the petitioners.

109. It will be noticed that Section 69A unlike Section 66A is a narrowly drawn provision with several safeguards. First and foremost, blocking can only be resorted to where the Central Government is satisfied that it is necessary so to do. Secondly, such necessity is relatable only to some of the subjects set out in Article 19(2). Thirdly, reasons have to be recorded in writing in such blocking order so that they may be assailed in a writ petition under Article 226 of the Constitution.

110. The Rules further provide for a hearing before the Committee set up - which Committee then looks into whether or not it is necessary to block such information. It is only when the Committee finds that there is such a necessity that a blocking order is made. It is also clear from an examination of Rule 8 that it is not merely the intermediary who may be heard. If the "person" i.e. the originator is identified he is also to be heard before a blocking order is passed. Above all, it is only after these procedural safeguards are met that blocking orders are made and in case there is a certified copy of a court order, only then can such blocking order also be made. It is only an

intermediary who finally fails to comply with the directions issued who is punishable under sub-section (3) of Section 69A.

111. Merely because certain additional safeguards such as those found in Section 95 and 96 CrPC are not available does not make the Rules constitutionally infirm. We are of the view that the Rules are not constitutionally infirm in any manner.

Section 79 and the Information Technology (Intermediary Guidelines) Rules, 2011.

112. Section 79 belongs to Chapter XII of the Act in which intermediaries are exempt from liability if they fulfill the conditions of the Section. Section 79 states:

> "79. Exemption from liability of intermediary in certain cases.—(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
> (2) The provisions of sub-section (1) shall apply if—
> (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
> (b) the intermediary does not—

(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission;
(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
(3) The provisions of sub-section (1) shall not apply if—
(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.
Explanation.—For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.]"

113. Under the 2011 Rules, by Rule 3 an intermediary has not only to publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource but he has also to inform all users of the various matters set out in Rule 3(2). Since Rule 3(2) and 3(4) are important, they are set out hereinbelow:-

“3. Due diligence to be observed by intermediary.—The intermediary shall observe following due diligence while discharging his duties, namely:—

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that—

(a) belongs to another person and to which the user does not have any right to;

(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

(c) harm minors in any way;

(d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(g) impersonate another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

> (i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.
>
> (4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through e-mail signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty-six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes."

114. Learned counsel for the petitioners assailed Rules 3(2) and 3(4) on two basic grounds. Firstly, the intermediary is called upon to exercise its own judgment under sub-rule (4) and then disable information that is in contravention of sub-rule (2), when intermediaries by their very definition are only persons who offer a neutral platform through which persons may interact with each other over the internet. Further, no safeguards are provided as in the 2009 Rules made under Section 69A. Also, for the very reasons that Section 66A is bad, the petitioners

assailed sub-rule (2) of Rule 3 saying that it is vague and over broad and has no relation with the subjects specified under Article 19(2).

115. One of the petitioners' counsel also assailed Section 79(3)(b) to the extent that it makes the intermediary exercise its own judgment upon receiving actual knowledge that any information is being used to commit unlawful acts. Further, the expression "unlawful acts" also goes way beyond the specified subjects delineated in Article 19(2).

116. It must first be appreciated that Section 79 is an exemption provision. Being an exemption provision, it is closely related to provisions which provide for offences including Section 69A. We have seen how under Section 69A blocking can take place only by a reasoned order after complying with several procedural safeguards including a hearing to the originator and intermediary. We have also seen how there are only two ways in which a blocking order can be passed – one by the Designated Officer after complying with the 2009 Rules

and the other by the Designated Officer when he has to follow an order passed by a competent court. The intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69A read with 2009 Rules.

117. Section 79(3)(b) has to be read down to mean that the intermediary upon receiving actual knowledge that a court order has been passed asking it to expeditiously remove or disable access to certain material must then fail to expeditiously remove or disable access to that material. This is for the reason that otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not. We have been informed that in other countries worldwide this view has gained acceptance, Argentina being in the forefront. Also, the Court order and/or the notification by the appropriate Government or its agency must strictly conform to the subject matters laid down in Article 19(2). Unlawful acts beyond what is laid down in

Article 19(2) obviously cannot form any part of Section 79. With these two caveats, we refrain from striking down Section 79(3)(b).

118. The learned Additional Solicitor General informed us that it is a common practice worldwide for intermediaries to have user agreements containing what is stated in Rule 3(2). However, Rule 3(4) needs to be read down in the same manner as Section 79(3)(b). The knowledge spoken of in the said sub-rule must only be through the medium of a court order. Subject to this, the Information Technology (Intermediaries Guidelines) Rules, 2011 are valid.

119. In conclusion, we may summarise what has been held by us above:

(a) Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2).

(b) Section 69A and the Information Technology (Procedure & Safeguards for Blocking for Access of Information by Public) Rules 2009 are constitutionally valid.

(c) Section 79 is valid subject to Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material. Similarly, the Information Technology "Intermediary Guidelines" Rules, 2011 are valid subject to Rule 3 sub-rule (4) being read down in the same manner as indicated in the judgment.

(d) Section 118(d) of the Kerala Police Act is struck down being violative of Article 19(1)(a) and not saved by Article 19(2).

All the writ petitions are disposed in the above terms.

……..……...J.
(J. Chelameswar)

……..……...J.
(R.F. Nariman)

New Delhi,

March 24, 2015.

India's Surveillance State

sflc.in

WORLD WIDE WEB FOUNDATION

Communications Surveillance in India

Table of contents

List of statutes i
List of cases ii
List of abbreviations iii
1. Introduction 1
2. Enabling Statutes 3
2.1 Telephones 3
2.1.1 Procurement and review of lawful order under Rule 419A 5
2.1.2 Interception process under Rule 419A 6
2.2 Internet 8
3. Enabling License Agreements 15
3.1 Telephone tapping 17
3.2 Surveillance of Internet data 18
3.2.1 Obligations of ISPs under ISL 18
3.2.2 Obligations of ISPs under UL 19
3.3 Surveillance of Internet meta-data 19
4. Functional Surveillance Mechanisms 22
4.1 Lawful Interception and Monitoring systems 22
4.2 Centralized Monitoring System 24
4.3 Network Traffic Analysis 27
4.4 National Intelligence Grid 29
4.5 Unlawful interception and monitoring 30
5. Privacy: The Indian Perspective 32
6. Surveillance and Human Rights 35
7. The Necessary and Proportionate Principles 38
7.1 Legality 38
7.2 Legitimate aim 39
7.3 Necessity 40
7.4 Adequacy 40
7.5 Proportionality 41
7.6 Competent judicial authority 42
7.7 Due process 43
7.8 User notification 44
7.9 Transparency 44
7.10 Public oversight 45
7.11 Integrity of communications and systems 45
7.12 Safeguards for international cooperation 46
7.13 Safeguards against illegitimate access 47
8. Conclusion 49
Appendix 50

List of statutes

Indian Telegraph Act, 1885

Indian Telegraph Rules, 1951

Information Technology Act, 2000

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Information Technology (Intermediaries Guidelines) Rules, 2011

Information Technology (Guidelines for Cyber Cafe) Rules, 2011

Code of Criminal Procedure, 1973

List of cases

People's Union for Civil Liberties v. Union of India [AIR 1997 SC 568]

Rajeev Chandrasekhar v. Union of India [W.P.(C).No. 23 of 2013]

MouthShut.com v. Union of India [W.P.(C).No. 217 of 2013]

Kharak Singh v. State of Uttar Pradesh & Ors. [(1964) 1 SCR 332]

Govind v. State of Madhya Pradesh [(1975) 2 SCC 148]

R R Gopal & Anr. v. State of Tamil Nadu [(1994) 6 SCC 332]

Ratan Tata v. Union of India [W.P.(C).No. 398 of 2010]

List of abbreviations

C-DOT	Centre for Development of Telematics
CAIR	Centre for Artificial Intelligence and Robotics
CCA	Controller of Certifying Authorities
CCPR	Centre for Civil and Political Rights
CBDT	Central Board of Direct Taxes
CBI	Central Bureau of Investigation
CDR	Call Data Record
CMS	Centralized Monitoring System
CrPC	Criminal Procedure Code
DIA	Defense Intelligence Agency
DOT	Department of Telecommunications
DRDO	Defense Research and Development Organization
DRI	Directorate of Revenue Intelligence
ED	Enforcement Directorate
GB	Giga-byte
GoI	Government of India
GPS	Global Positioning System
HCHR	High Commissioner on Human Rights
HRC	Human Rights Commission
IB	Intelligence Bureau
ICCPR	International Covenant on Civil and Political Rights
IP	Internet Protocol
IPDR	Internet Protocol Data Record
IPTV	Internet Protocol Television
ISF	Information Store and Forward
ISL	Internet Service License
ISP	Internet Service Provider
IT Act	Information Technology Act

TRAI	Telecom Regulatory Authority of India
TSP	Telecom Service Provider
UASL	Unified Access Service License
UDHR	Universal Declaration on Human Rights
US	United States
UL	Unified License
UN	United Nations

1. Introduction

In June 2013, the world was treated to a rude awakening by a hitherto unknown Edward Snowden, when he made public thousands of classified documents that belonged to the United States' National Security Agency (NSA). Described as one of the most significant leaks in US history, the disclosed documents revealed that the US Government had been discreetly collecting unprecedented quantities of surveillance data on everyone from its own citizens to foreign Governments, ostensibly as part of its global war against terror.

While most of the rest of the world was foreseeably outraged by the contents of Snowden's revelations, the then Indian Government's response to the matter was tepid at best, and the whole affair was shrugged off as a routine occurrence in international diplomacy. This stand was especially surprising since India, who has always boasted friendly ties with the US, was reportedly fifth in the overall list of countries spied on by the NSA programs. Why then was India rushing to the US' defense, with the then Minister for External Affairs going so far as to say that the US surveillance programs are "not actually snooping"?

On closer inspection, one quickly begins to realize that the Government of India's (GoI) tolerance of US surveillance might have been brought on by more than a mere desire to keep Indo-US relations from going sour. In line with the age-old adage against throwing stones in a glass house, the Government's remarkable restraint might have stemmed – at least in part – from the fact that it was busy with some "snooping" of its own. While we note with great satisfaction the earnest words of the current Minister of External Affairs, Ms. Sushma Swaraj on issues of US surveillance and hope the matter will get the attention it deserves, the need to understand India's domestic surveillance practices is not obliterated.

> Multiple Indian legislations ... contain explicit provisions that allow Central and State Governments to intercept and monitor the nation's communication networks on several grounds.

Multiple Indian legislations, including the Indian Telegraph Act and Rules, Information Technology Act and Rules and the Code of Criminal Procedure, contain explicit provisions that allow Central and State Governments to intercept and monitor the nation's communication networks on several grounds. These grounds are often broadly worded, with generous helpings of terms such as 'security of the state' and 'public safety' that are never defined with any manner of precision. This effectively grants the Government unsubstantiated access to India's telephone and Internet networks to retrieve their contents at will. Similarly, license agreements entered into between Indian communications service providers and the Department of Telecommunications contain clauses that mandate *inter alia*, the installation of unspecified surveillance equipment into communication networks as and when required by the Government and its

agents. All service providers operating within the country at any given point of time are therefore bound to ensure that their networks are open to Government surveillance.

Under the authority of the aforementioned provisions of law, a number of Lawful Interception and Monitoring (LIM) systems have been installed into India's telephone and Internet networks. These bare in real-time our phone calls, texts, e-mails and general Internet activity to Government surveillance. 'LIM systems' being a generic term that alludes to any surveillance system sanctioned by law, the true nature and extent of capabilities of the specific systems employed by the Indian Government remain matters of intelligent speculation. Aside from these pre-existing LIM systems, a slew of additional surveillance systems designed to significantly enhance the Government's existing capabilities are also in the pipeline in varying stages of deployment. This includes as of current knowledge, the Central Monitoring System (CMS), Network Traffic Analysis (NETRA), and National Intelligence Grid (NATGRID) – all of which will be examined in detail in the course of this report.

An application filed by SFLC.in under the Right to Information Act revealed that on an average, around *7500 – 9000* telephone-interception orders are issued by the Central Government alone *each month*. Extrapolating this number to include all interception orders issued by the Central and State Governments combined, it becomes clear that Indian citizens are routinely and discreetly subjected to Government surveillance on a truly staggering scale.

In this report, SFLC.in delves into the unchartered wilderness that is India's surveillance landscape in a pragmatically pessimistic bid to demystify our surveillance practices. In order to keep the scope of research within the realm of feasibility, this report will restrict itself to Indian *communications* surveillance i.e. surveillance of telephones and the Internet. In this regard, we will take an in-depth look at various aspects of India's surveillance machinery, including enabling provisions of law, service provider obligations, and known surveillance mechanisms. We will offer recommendations aimed at bettering what our readers will hopefully see is a lamentable state of affairs.

We express our sincere gratitude to the Web We Want campaign, without whose invaluable contributions this report would not have been possible.

2. Enabling Statutes

It is only fitting that any study of India's communications surveillance landscape commence with the various provisions of law whence the Government derives its broad powers. Accordingly, we now turn to statutes that enable surveillance of the two most widely subscribed modes of communication and information exchange in India *viz.* telephones and the Internet.

2.1 Telephones

When it comes to surveillance of telephone networks, the **Indian Telegraph Act, 1885** serves as the primary enabling statute. The definition of the term "*telegraph*" as provided under **Section 3(1AA)** of the Act goes above and beyond its linguistic connotations, 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 device – including telephones – within the Act's purview.

> The occurrence of a public emergency or the interest of public safety are therefore pre-requisites for the invocation of Section 5(2)

Going forward, **Section 5(2)** of the Telegraph Act provides for telephone tapping by the Government. It reads:

"*On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order.*"

The occurrence of a public emergency or the interest of public safety are therefore pre-requisites for the invocation of Section 5(2). In the absence of either, the Government is disallowed from intercepting communications made over telephones. While the terms 'public emergency' and 'public safety' are not defined under the Act itself, they were interpreted by the Supreme Court of India in the matter of *People's Union for Civil Liberties v. Union of India*[1] 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.

To recap, if either of the above conditions

1 AIR 1997 SC 568

are met, Central/State Governments or any of their authorized officers may direct that communications made over telephones be intercepted, if such interception is considered necessary or expedient in the interest of:

- Sovereignty/integrity of India
- Security of the State
- Friendly relations with foreign States
- Public order
- Prevention of incitement to the commission of any offence

None of the above five expressions have been defined under the Telegraph Act, which means they are open to interpretation by the concerned authority that sanctions interception.

With the *substantive* law regarding telephone tapping laid out by Section 5(2), the *procedural* law regarding the same is found under **Rule 419A** of the **Indian Telegraph Rules, 1951**. It is important to note that Rule 419A was not part of the Telegraph Rules when they were originally notified in 1951. It was introduced by way of an amendment in 2007, which was necessitated by the Supreme Court's condemnation in PUCL[2] of the lack of procedure governing telephone tapping. Due to this absence of procedure, the Supreme Court in PUCL had also enumerated certain guidelines to be followed while intercepting communications under Section 5(2). These guidelines served as a place-holder up until 2007, when Rule 419A was officially added to the Telegraph Rules, replacing the Court-issued guidelines.

As the procedure laid down by Rule 419A is lengthy and complicated to say the least, it will be examined in two phases – (1) procurement and review of lawful order, and (2) interception process.

2 Supra. 1

2.1.1 Procurement and review of lawful order under Rule 419A

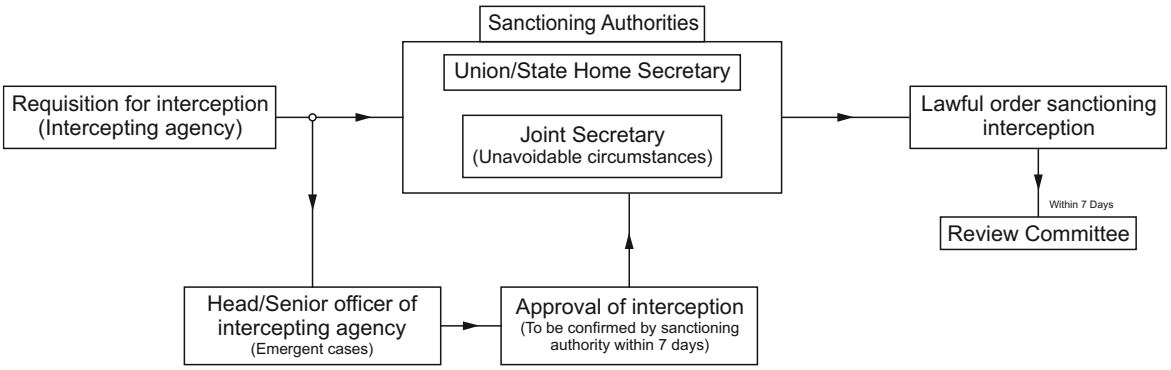


Fig. 1 – Procurement and review of lawful order

According to Rule 419A, a direction for interception under Section 5(2) [hereinafter referred to as the 'lawful order'] may normally be issued only by the Union Home Secretary at the Centre, or a State Home Secretary at the States. However, in *unavoidable circumstances*, a lawful order may be issued by an officer not below the rank of a Joint Secretary to the Government of India, who has been authorized by the Union/State Home Secretary to this effect.

> Rule 419A also states that a lawful order may be issued only once all other reasonable means for acquiring the information have been considered and ruled out.

Now the term "unavoidable circumstances" has not been defined under the Telegraph Rules, Telegraph Act, any other legislation, or judgments by courts of law. As a result, there exists no objective standard to determine whether a given situation qualifies as an unavoidable circumstance. This raises the very pertinent question: who decides whether a circumstance is unavoidable and how?

Setting aside this unresolved ambiguity in procedure, Rule 419A stipulates another exception to the general rule. In *emergent cases*, where procuring a lawful order is itself infeasible – either due to remoteness of location, or for operational reasons, interception may be carried out with the prior approval (as distinct from lawful order) of the Head or the second senior most officer of the authorized Law Enforcement Agency at the Centre, or officers authorized in this behalf – not below the rank of Inspector General of Police – at the States.

This exception to the general rule operates at the implementational level of interception, and says that if it is not possible to procure a lawful order for either of the listed reasons, the interception process may commence even without a lawful order as long as it is approved by a senior official as specified of the intercepting agency. However, when

interception is carried out in this fashion, the relevant sanctioning authority – be it a Union/State Home Secretary (or possibly a Joint Secretary) – must be informed of the fact within 3 working days, and the lawful order itself must be procured within 7 working days. Failing this, all interception must cease from the 8th day, until a lawful order is procured from the concerned sanctioning authority.

Rule 419A also states that a lawful order may be issued only once all other reasonable means for acquiring the information have been considered and ruled out. Any order so issued will remain in force for a period of 60 days from the date of issue, unless revoked earlier. Though the order may subsequently be renewed if necessary, no order will remain in force for more than a sum total of 180 days. All lawful orders must further contain:

• reasons behind the order, and;

• name and designation of the authority to whom the intercepted information is to be disclosed, and;

• a statement to the effect that the use of intercepted information will be subject to Section 5(2) of the Telegraph Act.

When a lawful order is issued by any of the concerned authorities, a copy must be forwarded within 7 working days to the respective Central/State Review Committee, which has been constituted by the Central/State Government under Rule 419A for the sole purpose of reviewing lawful orders. The constitution of Review Committees, though entirely Executive in nature, differs depending on whether it is a Central or State Review Committee. A Central Review Committee will consist of the Cabinet Secretary as Chairman, and the Secretary to the Government of India In-charge, Legal Affairs and the Secretary to the Government of India, Department of Telecommunications as Members. A State Review Committee on the other hand, will consist of the Chief Secretary as Chairman, and the Secretary Law/Legal Remembrancer In-charge, Legal Affairs and a Secretary to the State Government (other than the Home Secretary) as Members.

Review Committees will meet at least once in 2 months and determine if the lawful orders placed before them are in accordance with Section 5(2) of the Telegraph Act. When a Committee is of the opinion that a lawful order is violative of Section 5(2), it may set aside the order and ask that all copies of information intercepted under that particular order be destroyed.

2.1.2 Interception process under Rule 419A

Now that we have seen how a lawful order is procured and reviewed under Rule 419A, we turn to the process of interception itself. Procedure in this regard must be adhered to at all times, even if interception is undertaken in unavoidable or emergent circumstances.

The actual ground-level interception of communications over telephones will be carried out by various Law Enforcement Agencies such as the Intelligence Bureau and the Research and Analysis Wing, which have been specifically authorized

to this effect by the Government. However, the identities of agencies so authorized are not disclosed to the public for security reasons.

In any case, as per Rule 419A, all intercepting agencies will designate one or more nodal officers to authenticate and relay requisitions for interception between the agencies and Telecommunications Service Providers. These nodal officers will be senior officials of the agencies, not below the rank of (Additional) Superintendent of Police or equivalent. The TSPs in turn will designate two senior officials as nodal officers to receive and handle requisitions. Requisitions (which will include lawful orders authorizing interception) will be delivered to nodal officers of the respective TSPs by officers not below the rank of Sub-Inspector of Police, and the nodal officers will issue letters of acknowledgement to the relevant intercepting agencies within 2 hours of their reception.

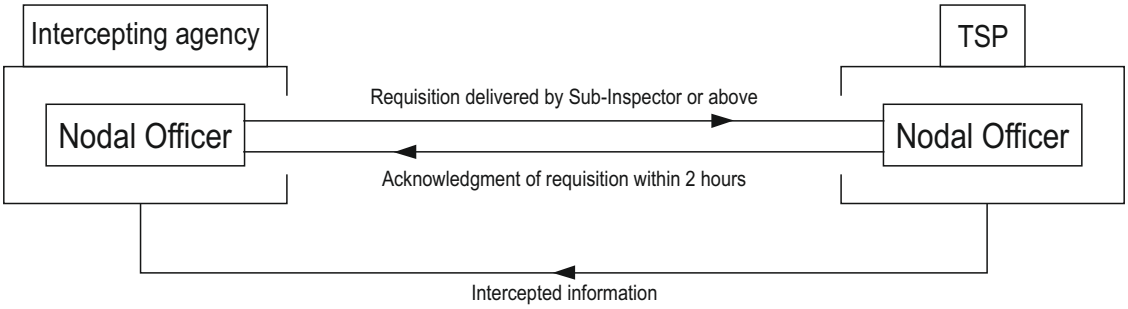


Fig. 2 – Interception process

Here ends the procedure detailed by Rule 419A with respect to the interception process. Internal protocol to be followed by both intercepting agencies and TSPs in handling requisitions for interception,

which presumably explains how intercepted information finds its way to the intercepting agencies, are further enumerated by periodic guidelines or notifications issued by the Central Government in the form of Standard Operating Procedures. However,these SOPs are kept out of public reach for security reasons, thereby ensuring that none other than those directly involved in the interception process have a comprehensive idea of the end-to-end procedure. An RTI request filed by SFLC.in seeking a copy of the latest of such SOPs was denied by the Department of Telecommunications, claiming exemption under Section 8(1)(a) of the RTI Act, which exempts the disclosure of information that may prejudicially affect national security.

Rule 419A does nevertheless go on to lay down certain procedural safeguards aimed at preventing misuse of intercepted information.

For starters, officers authorized to intercept are required at all times to maintain records that contain the intercepted information itself, particulars of interceptees, particulars of those to whom intercepted information has been disclosed, number of copies of intercepted information created, mode of creating said copies, date of destruction of said copies and duration for which the lawful order remained in force. TSPs in turn, are to put in place adequate and effective internal checks in order to ensure that unauthorized interception does not take place, and that extreme secrecy is maintained, and utmost care and precaution taken in the interception process. Further, TSPs are made responsible for the actions of their employees, and established violations of relevant license[3] clauses will result in action being taken against TSPs under the Telegraph Act, and this may even extend to revocation of their licenses. Last, but certainly not the least, all records pertaining to intercepted information are to be destroyed by sanctioning authorities and intercepting agencies every 6 moths, unless they (likely) need to be retained for "functional requirements". Similarly, TSPs are to destroy all such records 2 months after ceasure of interception, and are required to maintain extreme secrecy in doing so.

2.2 Internet

Provisions dealing with Internet surveillance may be found interspersed throughout the **Information Technology Act, 2000** and several Rules made thereunder.

But before looking at the enabling provisions themselves, a distinction must be made between "Internet data" and "Internet meta-data" – the two broad categories of electronic data, whose surveillance is provisioned by the below statutory clauses. The term "Internet data" connotes the core contents of data-packets transmitted between a user-end device and the host-server in which information accessed by the user resides. This would include the contents of

3 This refers to the service licenses granted to service providers by the Department of Telecommunications, which govern the general, technical, financial, operational and security conditions under which service providers must operate.

websites browsed, e-mails sent/received, chat-logs and so on. "Internet meta-data" on the other hand, signifies particulars of Internet data *apart from its core-contents*. This would include information such as date and time of transmission, duration for which data was transmitted and location from/to which data was transmitted.

With that out of the way, **Section 69** of the IT Act, modeled extensively after Section 5(2) of the Telegraph Act, allows the Government to engage in surveillance of Internet data. It reads:

> (1) *Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing the incitement to the commission of any cognizable offence relating to the above or for the investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.*
>
> (2) *The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.*
>
> (3) *The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to -*
>
> (a) *provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or*
>
> (b) *intercept, monitor, or decrypt the information, as the case may be, or;*
>
> (c) *provide information stored in computer resource*
>
> (4) *The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.*

As can be seen, Section 69 in provisioning surveillance of Internet data, draws much of its language from Section 5(2) of the Telegraph Act. The former, however, makes three notable departures from the latter. Firstly, Section 69 dispenses with the all-important *sine qua non* found under Section 5(2), *viz.* the occurrence of a public emergency or interest of public safety. Interception, monitoring, and decryption of Internet data under Section 69 is therefore not predicated on the prevalence of either pre-requisites, and this considerably widens the Govern-ment's

surveillance avenues when it comes to Internet data. Secondly, the grounds under Section 69, in the interest of which interception etc. of Internet data may be undertaken, is slightly larger in number and significantly greater in scope, as evidenced by the comparative table given below:

Grounds under Section 5, Indian Telegraph Act	Grounds under Section 69, Information Technology Act
Sovereignty/integrity of India	Sovereignty/integrity of India
-	Defence of India
Security of the State	Security of the State
Friendly relations with foreign States	Friendly relations with foreign States
Public order	Public order
Prevention of incitement to the Commission of any offence	Prevention of commission of any cognizable offence relating to the above
-	Investigation of any offence

Table 1 – Grounds for interception under Section 5(2), Telegraph Act and Section 69B IT Act

Lastly, unlike Section 5(2), Section 69 imposes an obligation on those from whom Internet data is demanded (Internet Service Providers, for instance) to provide all assistance to the intercepting agency, failure to comply with which may result in incarceration for up to *7 years* and fines.

With surveillance of the Internet data thus provisioned by Section 69, **Section 69B** in turn deals with surveillance of Internet meta-data. It reads:

> 1. *The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the*

Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

2. *The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.*

3. *The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.*

4. *Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.*
Explanation: For the purposes of this section,

i) *"Computer Contaminant" shall have the meaning assigned to it in Section 43*

ii) *"traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.*

Section 69B allows the collection and monitoring of meta-data – cloaked as "traffic data" - for the twin purposes of enhancing cyber security and tackling computer contaminants. The term "cyber security" has been defined under Section 2(1)(nb) of the IT Act as the protection of information or devices from unauthorized access, use, disclosure, disruption, modification or destruction, and the term "computer contaminants" as per Section 43 of the IT Act denotes malicious software such as computer viruses. Both grounds for invocation of Section 69B are visibly broad in ambit, and essentially allow surveillance of meta-data at any given point of time.

The procedure to be followed while invoking Sections 69 and 69B are laid down under the **Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009**, and the **Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009**. The procedure outlined by these Rules are near-identical replications of the procedure under Rule 419A of the Telegraph Rules, and their reiteration here is therefore unnecessary for the purpose of this report. It would suffice to keep in mind that Internet surveillance is governed by the same broad procedural framework as telephone surveillance.

While Sections 69 and 69B together set the stage for direct surveillance of Internet networks, more provisions of the IT Act allow indirect surveillance i.e. they allow

the Central/State Governments and their agents such as the Controller of Certifying Authorities and police officers to collect "information" under specified circumstances. In the absence of clarifications on the nature of information that can be collected, these provisions serve as alternate means to collect Internet data and meta-data when surveillance by means of Sections 69 and 69B may not be feasible:

• **Section 28** of the **Information Technology Act** allows Government officials to access any electronic data while investigating contraventions of the Act and Rules or regulations made under the Act. The Section states that the Controller of Certifying Authorities (CCA) or any authorized officer may direct production of information towards investigating contraventions of the Act or connected Rules and regulations. It confers on them the powers of Income-tax authorities as under *Chapter XIII of the Income Tax Act, 1961* for the purposes of such investigation. Chapter XIII of the Income Tax Act awards the authorities significant powers of investigation, including the power to compel production of information stored electronically. Thus, the CCA in effect has the same authority under Section 28, provided such authority is exercised in the course of investigating a contravention of the IT Act.

In 2011, the CCA had imposed a fine on Yahoo! To the tune of Rs. 11 lakhs for its refusal to provide user information requested under Section 28. An interim order staying the fine was issued by the Delhi High Court in 2011, and a final order setting aside the fine was issued in February 2014.

Further, a Right to Information request filed by SFLC.in revealed that the CCA had made 73 requests for information in 2011 under Section 28.

• **Section 29** of the **Information Technology Act** provides the CCA or authorized officers with the power to access computers and their data on a *reasonable cause* to suspect contravention of Chapter VI of the Act. Chapter VI deals with regulation of Certifying Authorities and contains a number of provisions, whose contravention could be easily and reasonably suspected. Since no framework for the access of computers and data has been prescribed by the Section, it is frighteningly easy for Section 29 to be wrongfully invoked to access private user information from Certifying Authorities.

• **Rule 6** of the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**, says that though a body corporate is disallowed from disclosing sensitive personal data or inform-

ation to third parties without the prior consent of the provider of the information, it may disclose the same to Government agencies mandated under law without prior consent for the purpose of identity verification, prevention, investigation of offences etc. It further states that any sensitive personal data or information shall be disclosed to third parties by an order under law, presumably without prior consent of the provider.

• **Rule 3(7)** of the **Information Technology (Intermediaries Guidelines) Rules, 2011**, requires that intermediaries such as ISPs and on-line portals must provide information or any assistance to authorized Government agencies for the purpose of identity verification, prevention or investigation of offences etc., when asked to do so by a lawful order. There is some confusion here regarding the term 'lawful order' since the Rule uses it interchangeably with the term 'request in writing'. This seemingly implies that a 'lawful order' as envisioned under the Rule is nothing more than a written letter from authorized Government agencies, which does not bear adequate force of law. As a result, the process of directing the production of information under Rule 3(7) is inordinately simplified, and this is evident in general practice. The constitutionality of this provision was challenged by Yahoo in a Writ Petition[4] filed before the Delhi High Court, following the imposition of a hefty fine for refusal to provide information to the CCA under Section 28 of the IT Act. Though the fine itself was set aside by the Court, larger questions of law such as the constitutionality of Rule 3(7) were left undecided. The Rule has also been challenged before the Supreme Court in the cases of Rajeev Chandrashekhar v. UoI[5] and MouthShut.com v. UoI[6] as being violative of the citizens' right to privacy. Both cases are currently pending before the Supreme Court, awaiting judgement.

• **Rule 7** of the **Information Technology (Guidelines for Cyber Cafe) Rules, 2011**, states that an officer authorized by the registration agency, is authorized to check or inspect the cyber cafe and the computer resource or network established therein at any time for the compliance of these rules. The cyber cafe owner shall provide every related document, registers and any necessary information to the inspecting officer on demand. This is especially interesting, considering that cyber cafes are also classified as intermediaries under the IT Act. Thus, Rule 7 can be used to access personal information from cyber cafes including Internet histories

4 W.P.(C).No. 6654/2011
5 W.P.(C).No. 23 of 2013
6 W.P.(C).No. 217 of 2013

and other user-related information.

Apart from the IT Act and Rules, **Section 91** of the **Code of Criminal Procedure, 1973** (CrPC) says that any Court or officer in charge of a police station may require the production of any document or 'other thing' if it is considered necessary for the purposes of an investigation, inquiry, trial or any other proceeding under the CrPC. Since this is the legislation which the police authorities are familiar with, it is often found that requisitions sent to intermediaries directly by the police often ask for information based on Section 91. For instance, a vernacular blog *bodhicommons.org* was issued a notice in February 2013 under Section 91 based on a complaint made by a regional media house *Mathrubhumi*, where the blog was asked to remove an allegedly defamatory post containing discussions on unfair labour practices at *Mathrubhumi*. The notice also directed bodhicommons to furnish registration details of the URL (sic) from which the offending post was originally made. Again, a consumer review website *mouthshut.com* was issued notices under Section 91 demanding identification details regarding the up-loaders of several unfavourable reviews found on the website.

Thus the above-mentioned provisions of law collectively enable the Government and its agents to surveil India's telephone and Internet networks on a variety of grounds. However, these are not the only sources from where such authority is derived. In addition to legislations, surveillance-enabling clauses/conditions are also found across several service license agreements, which are discussed in the following pages.

Since this is the legislation which the police authorities are familiar with, it is often found that requisitions sent to intermediaries directly by the police often ask for information based on Section 91.

3. Enabling License Agreements

Having seen the surveillance-enabling provisions found across Indian legislations, we turn to more enabling clauses – found this time around in license agreements between the Department of Telecommunications (DOT) and communications service providers. The DOT is an executive organ of the Ministry of Communications and Information Technology, and is the prime regulator of Indian communications service industry. The aforementioned license agreements in their various iterations, govern provision of the following services:

- Fixed-line telephones
- Cellular/mobile telephones
- Internet
- Satellite communications
- Two-way radios
- Private leased circuits

These license agreements are essentially what allow service providers to conduct their businesses in India, and accordingly they detail the various general, commercial, financial, operational, technical and security conditions under which they must operate. Licensees are under a legal obligation to abide by all said conditions, failing which their licenses may be revoked. But before getting into the surveillance-enabling clauses, some background information on the license agreements themselves is in order.

Prior to 2003, the Indian communication service licensing regime was fragmented into multiple individual licenses, with separate licenses for each kind of communication service mentioned above. However, it was recognized in the New Telecom Policy (NTP) of 1999 that the ongoing convergence of markets and technologies called for a realignment of this licensing model. While technology was busy blurring the lines of differentiation among conduit systems, various service providers were already entering one another's markets. In view of such fundamental shifts in the telecom service paradigm, the Telecom Regulatory Authority of India (TRAI) recommended the consolidation of the fragmented individual licenses into a single unified model. Though the key objective of the proposed unified licensing model was to encourage free growth of new applications and services leveraging the technological advancements, it also had the following ancillary objectives:

- Simplification of licensing procedure
- Ensuring flexibility and efficient utilization of resources
- Encouraging efficient small service providers to cover niche areas, particularly rural and remote areas where telecom penetration was insufficient
- Ensuring easy entry, level playing field and 'no-worse-off' situation for existing service providers

With these objectives in mind, the consolidation of licenses was kicked off in 2003 in two phases:

- The first phase introduced the Unified Access Service License (UASL) merging license agreements covering provision of fixed-line and cellular/mobile telephone telephone services.

- The second phase introduced the Unified License (UL) as part of the New Telecom Policy of 2012, which merged *all* service licenses into one umbrella license.

However, migration to the new UL has been prescribed on a voluntary basis and thus, while subscribers to the erstwhile individual licenses have almost entirely migrated to the UASL, migration to the UL is still ongoing with only two service providers – Sistema Shyam Teleservices (operating under the brand name MTS) and Reliance Jio Pvt. Ltd. - currently subscribed to the UL.

Since the scope of this report is Indian surveillance of *mainstream* communications, its focus will be on the license agreements currently governing provision of fixed-line/mobile telephone and internet services, namely:

- Unified Access Service License (UASL)

- Internet Service License (ISL)

- Unified License (UL), particularly Chapters VIII and IX of Part II, which incorporate the above-two licenses into the UL

All of the above-mentioned license agreements require their licensees to furnish 'all necessary means and facilities as required' for the application of Section 5[7] of the Indian Telegraph Act[8]. Licensees must also provide in the interests of security, 'suitable monitoring equipment' as per the requirement of the DOT or LEAs[9]. The specific orders or directions from the Government issued under such conditions (i.e. in the interests of security) are also applicable[10]. Further, licensees are obliged to provide all tracing facilities to trace nuisance and obnoxious/ malicious communications passing through their networks, when such information is required for investigations or detection of crimes, and in the interest of national security[11]. They must also provide 'necessary facilities' depending upon the specific situation at the relevant time, to counteract espionage, subversive act, sabotage or any other unlawful activity[12].

Thus under the afore-mentioned clauses, licensees may be asked to provide surveillance equipment in any *one* of the following scenarios:

- Situations where Section 5 of the Indian Telegraph Act is applicable

- In the interests of (national)

7 See p. 3
8 Clause 32.2, UASL; Clause 35.2, IL; Condition 32.2, Part I, UL
9 Clause 41.13, UASL; Clause 34.4, IL; Condition 39.12, Part I, UL
10 Ibid.
11 Clause 40.4, UASL; Condition 38.2, Part I, UL
12 Clause 41.1, UASL; Condition 39.1, Part I, UL

security

- For the investigation/detection of crimes

- To counteract:

  - Espionage
  - Subversive acts
  - Sabotage
  - Any other unlawful activity

Terms such as national security, espionage, subversive acts and sabotage are not defined anywhere in the license agreements, enabling the Government to call for the installation of surveillance equipment with no accompanying obligation to clearly outline reasons for the same.

It is also interesting to note that the nature of surveillance equipment to be provided is not mentioned under the licenses. Instead, open-ended terms such as 'necessary means and facilities', 'suitable monitoring equipment' and 'tracing facilities' are liberally employed, which may signify virtually *any* surveillance equipment depending on the need of the hour and the state of technological progress.

That being said, the licenses do however specify the following details regarding surveillance systems, depending on their functionality:

3.1 Telephone tapping

Designated Central/State Government officials, apart from the DOT and its nominees, may access telephone-tapping systems installed into the licensees' networks.[13] Whereas the hardware belonging to such systems at the licensees' end, as well as all related software must be engineered, installed and maintained by the licensees at their own cost,[14] the cost of user-end hardware and leased line circuits to the monitoring centers will be borne by the respective Government agency. These monitoring centres may be located in the Government agencies' premises or in the premises of the licensees.[15] In the latter case, licensees should extend all support in this regard including Space and Entry of the authorized security personnel.[16]

Further, Licensees should make arrangements for monitoring simultaneous calls by Government security agencies.[17] The number of simultaneous calls to be monitored has been given to be 480, with at least 30 for each of the 10 currently designated security agencies.[18] Identities of the specific designated agencies are unknown at this time as this information is provided directly to the service providers and agencies in the form of periodic (publicly inaccessible) guidelines. Additionally, each of the licensees' Mobile Switching Centres must have the capacity to provision at least 3000 numbers for monitoring.[19]

13 Clause 41.16, UASL; Condition 8.2, Part II, Chapter VIII, UL
14 Ibid.
15 Clause 41.16, UASL; Condition 8.2, Part II, Chapter VIII, UL
16 Ibid.
17 Supra. 7
18 Supra. 9
19 Supra. 9

Along with the monitored calls, the following records must also be made available:[20]

- Called/calling party mobile /PSTN numbers
- Time/date and duration of interception
- Location of target subscribers. For the present, Cell ID should be provided for location of the target subscriber. However, Licensor may issue directions from time to time on the precision of location, based on technological developments and integration of Global Positioning System (GPS) with Cellular Network, which shall be binding on the licensee.
- Telephone numbers if target subscriber has invoked any call-forwarding features
- Data records for even failed call attempts
- CDR (Call Data Record) of Roaming Subscriber

3.2 Surveillance of Internet data

Clauses dealing with surveillance of Internet data see some variation between the ISL and the UL.

3.2.1 Obligations of ISPs under ISL

> Under the ISL, ISPs are required to maintain copies of all packets originating from their equipment such as modems or routers located on the customers' premises, and these must be available in real time to the Telecom Authority

Under the ISL, ISPs are required to maintain copies of all packets originating from their equipment such as modems or routers located on the customers' premises, and these must be available in *real time* to the Telecom Authority[21].[22] Further, every international gateway location and/or ISP node with a router/switch having an outbound capacity of 2 Mbps or more must be equipped with a monitoring center at the cost of the ISP.[23] 'Suitable monitoring systems' must also be set up by ISPs carrying Internet telephony traffic through their internet gateways and/or ISP nodes at their own cost, as per the requirement of the security agencies, and the cost of maintenance of the monitoring equipment and infrastructure at the monitoring center located at the premises of the licensee shall be borne by the ISP.[24] For a national ISP or an ISP having multiple nodes/points of presence, a central monitoring center would be acceptable. However in such a case, the ISP should demonstrate to the DOT that all routers/switches are accessible from the

20 Clause 41.17, UASL; Condition 8.3, Part II, Chapter VIII, UL
21 Denotes the Director General, Telecommunications, Government of India and includes any officer empowered by him to perform all or any of the functions of the Telegraph Authority under the Indian Telegraph Act, 1885 or such other authority as may be established by law
22 Supra. 13
23 Clause 34.27, ISL
24 Ibid.

central monitoring center. Moreover, the ISPs should inform the DOT of every change that takes place in their topology/configuration, and demonstrate that all routers/switches continue to be accessible from the central monitoring center.[25] At locations where the ISP node has a router/switch with an outbound capacity of less than 2 Mbps, monitoring equipment will be provided by the security agencies.[26]

3.2.2 Obligations of ISPs under UL

The UL one the other hand requires ISPs to provide copies of customers' packets to the DOT or security agencies, as opposed to the Telecom Authority.[27] Further, 'suitable monitoring systems' for internet traffic – including internet telephony – flowing through the licensees' internet gateways/ISP nodes are to be set up by the licensees at their own cost as per the requirement of the DOT or security agencies.[28] The cost of maintenance of the monitoring equipment and infrastructure at the monitoring centers located at the premises of the licensees shall be borne by the licensees.[29] Licensees, while providing downstream Internet bandwidth to an ISP, should ensure that all the traffic of such ISPs passing through their networks can be monitored in the networks of the licensees.[30] However, licensees having upstream bandwidth from multiple service providers may be mandated to install monitoring systems at their ISP nodes as per the requirement of security agencies. In such cases, upstream service providers are not required to monitor this bandwidth.[31] The UL also makes the option of having one centralized monitoring center as opposed to multiple centers available to all ISPs having multiple nodes/points of presence, irrespective of whether they are national or international ISPs.

3.3 Surveillance of Internet metadata

Both the UASL and the UL require their licensees to archive all commercial records/Call Data Records/Exchange Data Records/IP Data Records with regards to communications exchanged in their networks for a period of one year for security reasons.[32] While the specific contents of these Data Records are unspecified, they may be destroyed thereafter unless otherwise directed by the DOT.[33] Interestingly though, the ISL in particular makes no mention of IP Data Records. However, IP Data Records would need to be archived by ISPs subscribed to the UL.

Further, licensees operating under the UASL and UL must be able to provide the geographical location of any subscriber (Base Transceiver Station location, and location details including latitude &

25 Supra. 23
26 Supra. 19
27 Condition 7.3, Part II, Chapter IX, UL
28 Condition 8.1.1, Part II, Chapter IX, UL
29 Ibid.
30 Condition 8.2, Part II, Chapter IX, UL
31 Condition 8.3, Part II, Chapter IX, UL
32 Clause 41.23, UASL;
33 Ibid.

longitude details) on request by the DOT or its authorized agencies.[34] They must also provide location details of mobile customers in licensed service areas as per the below-mentioned accuracy and time frame from the effective date of licenses:[35]

Accuracy in percentage							
Distance in meters	Urban (More than 1 million mobiles in a municipal limit)		Sub-urban and rural			Remote	
	1 year	2 years	1 year*	2 years	3 years	2 years	3 years
50	30	50					
100	60	75		50	60		-
300	80	95	50	60	70	50	60
500			60	70	80	60	70

Table 2 – Accuracy and time frame for collection of location details

To start with, these details need be provided only for specified mobile numbers - however, within a period of 3 years from effective date of license, they shall be part of CDR for *all* mobile calls.[36] Also, depending on technological development, these limits of accuracy can be modified by the DOT at any time.[37] Once again, the ISL makes no mention of location details in particular, but they would need to be provided by ISPs operating under the UL.

However, ISPs operating under the ISL are required to maintain logs of all users connected and the service they are using (mail, telnet, http etc.). They must also log every outward login or telnet through the connected users' computers. These logs must be available in *real time* to the Telecom Authority, and anonymous

34 Clause 41.26(x), UASL; Condition 39.23(x), Part I, UL
35 Clause 41.12, UASL; Condition 8.5, Part I, UL
36 Supra. 29
37 Ibid.

logins by users are not allowed.[38] The UL further mandates ISPs to maintain CDR/IPDR for Internet including Internet Telephony Service for a minimum period of one year.[39] Parameters of IPDR must be maintained as per the instructions issued by the DOT from time to time.[40] ISPs operating under the UL are also to maintain log-in/log-out details of all subscribers for services provided such as internet access, e-mail, Internet Telephony, IPTV etc. These logs shall again be maintained for a minimum period of one year.[41]

This just about sums up the license agreement clauses that provision direct surveillance of the nation's communication networks. As previously mentioned, the specific surveillance systems/ technologies to be employed by service providers are left unmentioned, and the license agreements settle instead for delineating the nature of information to be supplied and the manner in which they must be supplied. The Government agencies are then free to retrieve such information using the surveillance systems of their choice, depending on the state of technological progress and the availability of and need for said systems.

It is worth mentioning that the license agreements, apart from provisioning direct surveillance of communications, also contain certain provisions that quietly facilitate the Government's information gathering efforts. For instance, all licensees under all licenses discussed here are prohibited from employing bulk encryption equipment in their networks. Any encryption equipment connected to their networks for specific requirements need to be pre-evaluated and approved by the DOT.[42] The ISL in particular states that individuals, groups and organizations are permitted to use encryption only up to 40 bit key length in the symmetric key algorithms or its equivalent in other algorithms without obtaining permission from the DOT. If encryption equipment higher than this limit are to be deployed, they must obtain prior written permission of the DOT and deposit the decryption key, split into two parts, with the DOT.[43]

That said, we now move on to the actual surveillance systems employed by the Government of India – both the currently functional systems, as well as those in the pipeline.

38 Clause 34.8, ISL
39 Condition 7.1, Part II, Chapter IX, UL
40 Ibid.
41 Condition 7.2, Part II, Chapter IX, UL
42 Clause 39.1, UASL; Clause 2.2(vii), ISL; Condition 37.1, Part I, UL
43 Clause 2.2(vii), ISL

4. Functional Surveillance Mechanisms

Backed by legislations and license clauses, a host of surveillance systems perform the task of keeping a close tab on India's communication networks. Here we take a look at what is currently known regarding these systems – including their functionality and modes of operation. As a word of caution, said surveillance systems have been kept under tight wraps by the Government citing various security concerns, and reliable information on them is extremely difficult to come by in the public domain. While every effort has been made to source the facts detailed below from the most reliable of the available sources, they must nevertheless be regarded as involving a certain amount of speculation unless otherwise mentioned.

4.1 Lawful Intercept and Monitoring systems

Lawful Intercept and Monitoring systems – also known simply as Lawful Interception Systems (LIS) – generally refer to any legally approved surveillance system, public or private, that operate in a jurisdiction at a given point of time. However, in the context of this report, they may be understood to signify the interception/monitoring systems installed into the networks of TSPs/ISPs under the authority of the license agreements discussed in Chapter III. From a perusal of the relevant license clauses, it may be gathered that the collective body of LIM systems will be able to perform the following broad tasks:

- Intercept fixed-line/mobile/internet telephone calls
- Log and provide real time access to the entirety of Indian internet traffic
- Maintain and provide access to meta-data i.e. Call Data Records/Exchange Data Records/IP Data Records relating to the above, including, but not limited to the location of subscribers

Though the details on how these tasks are accomplished remain rather sketchy, a broad idea of the technology that powers LIM systems may be gleaned from the product portfolios of surveillance technology companies operating in India, who manufacture and distribute various lawful interception solutions aimed primarily at LEAs. Considering that selling surveillance technology to LEAs is clearly a viable business model, and that several key players from this industry have set up bases in India, a reasonable assumption can safely be made that such technology powers India's LIM systems at least in part. An RTI request filed by SFLC.in revealed a list of 26 companies that had expressed interest in placing bids on a tender calling for internet monitoring systems floated by the office of the Director General of Police, Logistics & Provisioning, New Delhi. Said companies are:

- Alcatel-Lucent India
- Agilis Information Technologies International
- Appin Software Security

- Aqsacom India
- ClearTrail Technologies
- Electronics Corporation of India Ltd., Information Technology & Telecom Division
- HCL Infosystems
- Hewlett-Packard India Sales
- Innefu Labs
- Intelligent Communication Systems India
- ITI
- Kommlabs Dezign
- Law Abiding Technology
- Narus Networks
- Netsweeper India
- NICE Systems
- Pyramid Cyber Security and Forensics
- Siemens Information Systems
- Span Technologies
- Span Telecom
- SS8 Network
- Telecommunications Consultants India
- Vehere Interactive
- Verient Systems India
- Vox Spectrum
- Xalted Information Systems

It can thus be safely definitively inferred that these 26 domestic as well as international companies already sell/are interested in selling internet surveillance technology to Indian LEAs. However, a look at their product portfolios – several of which have incidentally been published by WikiLeaks as part of *The Spy Files* initiative – will tell us that some of them also offer far more potent surveillance technologies including phone interception, social network analysis, and data-mining and profiling. However, there are no definite indicators as to which of the above-mentioned companies are active suppliers of surveillance equipment to Indian LEAs, and by extension, which specific technologies are in fact deployed.

... it is important to note that the operation of all LIM systems are bound by the procedural guidelines laid down by Section 5 of the Indian Telegraph Act read with Rule 419A of the Indian Telegraph Rules

That said, it is important to note that the operation of all LIM systems are bound by the procedural guidelines laid down by Section 5 of the Indian Telegraph Act read with Rule 419A of the Indian Telegraph Rules, where interception may only be

conducted in specified circumstances, and in pursuance of a lawful order issued by the competent authority on a case by case basis. The license agreements further mention 10 LEAs authorized to access LIM systems, though their identities are undisclosed. A report published by a national newspaper in June 2013[44] refer to the following nine LEAs as being authorized to "intercept and monitor citizens' calls and emails, under the guidelines laid down by the Supreme Court, The Indian Telegraph Act 1985, Rule 419(A) and other related legislation": Central Board of Direct Taxes (CBDT), Central Bureau of Investigation (CBI), Defense Intelligence Agency (DIA), Directorate of Revenue Intelligence (DRI), Enforcement Directorate (ED), Intelligence Bureau (IB), Narcotics Control Bureau (NCB), National Investigation Agency (NIA), Research and Analysis Wing (RAW), Military Intelligence of Assam and Jammu and Kashmir, and the Home Ministry. While by no means is this conclusive proof that these 9 LEAs are part of the 10 authorized LEAs mentioned in the license agreements, it would at least serve as an indicator of the nature of LEAs authorized in the usual course to conduct communications surveillance.

Thus, the majority of current Indian communications surveillance may be understood to be carried out by this existing framework of LIM systems. However, a number of additional surveillance systems in varying stages of development are currently in the works, including:

- The Centralized Monitoring System
- Network Traffic Analysis
- National Intelligence Grid

Unlike the current framework of LIM systems, a good portion of which may be privately sourced, these newer surveillance systems are engineered almost exclusively by various public R&D establishments such as the Defence Research and Development Organization (DRDO) or the Centre for Development of Telematics (C-DOT), and will work in tandem with the existing set up.

4.2 Centralized Monitoring System

Plans to set up the CMS were first announced in a November 2009 press release by the Press Information Bureau, where the then UPA Government notified its proposal to set up a centralized system to monitor communications on mobile phones, landlines and internet in the country.[45] As per the press release, the CMS was envisaged by the DOT to 'strengthen the security environment in the country'. It was said that with the CMS, the following inherent problems in the present system would be overcome:

- Easy compromise of secrecy due to manual intervention
- Considerable delay in interception process

44 http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece , accessed on December 14, 2013

45 http://pib.nic.in/newsite/erelease.aspx?relid=54679 , accessed on February 5, 2014

Additionally, the CMS was touted as having the following features:

- Central and regional database that will help Law Enforcement Agencies in interception and monitoring

- Direct Electronic Provisioning of target numbers by Government agencies without any manual intervention from the Telecom Service Providers

- Filters and alert creation on target numbers

- Call Data Records analysis and data mining on CDRs to identify call details, location details etc. of the target numbers

- R&D in related fields for continuous upgradation of the CMS

That said, it is important to note however that the CMS isn't a surveillance system *per se,* since the actual interception and monitoring of communications will still be carried out by the pre-existing framework of LIM systems. The CMS will primarily function in the capacity of an automated system of accessing information that has already been intercepted by LIM systems. For this purpose, it will have central and regional databases that will store intercepted data and provide access to LEAs authorized to use the CMS. But the CMS will be a massive step-forward from the existing surveillance framework, mainly due to its elimination of manual components from the interception chain of command. This automation of the interception process has two implications:

- LEAs using the CMS will no longer need to approach telecom/ internet service providers on a case-by-case basis to retrieve intercepted information

- The intercepted information will be delivered to LEAs instantaneously

The CMS will comb through information gathered to look for key words or phrases that have been flagged as indicative of unlawful activity and alert LEAs when such words/phrases are detected. Additionally, it will have CDR analysis and data-mining capabilities, which means it will also analyze meta-data to build speculative profiles of targeted individuals.

While it is thus clear that the CMS will have significant surveillance capabilities once fully functional, it is not intended to replace the existing LIM systems. The CMS' role will be restricted to the elimination of manual components in the information retrieval process and the consequent analysis of said information. To this end, the existing LIM systems will be linked to Information Store and Forward (ISF) servers belonging to the CMS, which will in turn be linked to the databases of CMS' Regional Monitoring Centers (RMC), which will finally feed into the CMS' central database, from where the

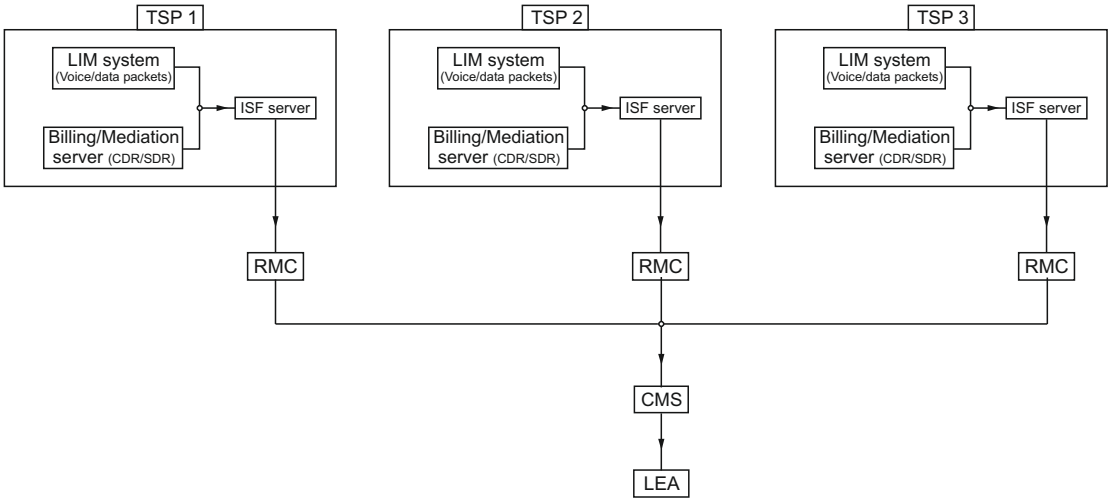


Fig. 3 – Collection of Information under Centralized Monitoring System

information will be accessed by authorized LEAs.[46]

In addition to the content of intercepted communications, the CMS will also have access to communications meta-data i.e. CDR and IPDR, which will be secured on multiple E1 leased lines through service providers' billing/ mediation servers.[47] In 2013, amendments were made to the Unified Access Service License and Unified License in order to connect the existing monitoring centers to the CMS network. Said amendments require service providers to provide dark optic fiber connectivity at their own cost up to the nearest point of presence of the CMS network. In case dark optic fiber connectivity is not readily available, (regular) optic fiber connectivity must be provided with 10 Mbps bandwidth upgradeable to 45 when required, but the switch to dark optic fiber must be made at the earliest.

As of June 2013, the following Government agencies are rumored to have been authorized to make intercept requests through CMS: Central Board of Direct Taxes (CBDT), Central Bureau of Investigation (CBI), Defense Intelligence Agency (DIA), Directorate of Revenue Intelligence (DRI), Enforcement Directorate (ED), Intelligence Bureau (IB), Narcotics Control Bureau (NCB), National Investigation Agency (NIA), Research and Analysis Wing (RAW), Military Intelligence of Assam and Jammu and Kashmir, and the Home Ministry.[48] While a majority of the RTIs filed by various organizations and individuals seeking to uncover information on the working of CMS were denied as the information was claimed to be protected under Section 8(1)(a) of the Right to Information Act, references were however made to *Rajya Sabha Unstarred Question No. 1598* and *Lok Sabha Unstarred Question No. 3207*, which revealed the following additional information:

46 http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece, accessed on Feruary 5, 2014
47 Supra. 45
48 Ibid.

• The CMS project was approved by the Cabinet Committee on Security in a meeting held on 16th July 2011.

• The interception and monitoring of any target under CMS can be done only after following the due process of law as stipulated in Section 5(2) of the Indian Telegraph Act read with Rule 419A of the Indian Telegraph Rules.

• CMS has an inbuilt mechanism of checks and balances, wherein the LEAs are unable to provision the targets themselves, and the provisioning authority is unable to see the content of the intercepted communication. Further, there is a provision of auto generation of audit trail of command logs related to interception and monitoring.

• The total fund allocation for CMS project is Rs. 400 crores. As on 12th December 2012, the expenditure incurred on R&D was Rs. 76.86 crores and on roll out of project, Rs. 4.25 crores.

• The development work of the system is largely completed. A pilot project was completed by 30th September 2011 at Delhi under which C-DOT installed two ISF servers – one each for Mahanagar Telephone Nigam Ltd. (MTNL) and Tata Communications Ltd. (TCL). The interception services were integrated and tested successfully for said service providers. Further, the system has been installed and integrated in Delhi License Service Area connecting six telecom service providers and one in Haryana License Service Area. The CMS has also been integrated with mobile number portability operators pan-India. Equipment was ordered for installation of CMS in six more Licensed Service Areas as on 12th December 2012.

However, while the interception process under the CMS is claimed to be governed by the procedure laid down by Section 5 of the Indian Telegraph Act read with Rule 419A of the Indian Telegraph Rules, the fact that the CMS is capable of Direct Electronic Provisioning of target numbers runs foul of said procedure since it dispenses with the chain of command involving manual elements such as nodal officers meant to authorize interception requests. Though this automation is said to better protect the privacy of citizens in terms of a reduction in the number of people in the know of whose/what communications are being monitored, it leaves no external non-governmental parties to verify the authenticity of interception requests. This undeniably makes clandestine/unauthorized surveillance by those so inclined a very real possibility.

4.3 Network Traffic Analysis

Though there have been earlier reports indicating its existence, the NETRA internet surveillance system [developed by Centre for Artificial Intelligence and Robotics (CAIR), a lab under Defence Research and Development Organization

(DRDO)[49]] was brought under the spotlight in earnest as recently as January 2014, when several Indian newspapers ran reports on its plans to monitor internet traffic for the use of words such as 'attack', 'bomb', 'blast' or 'kill' in tweets, status updates, emails or blogs. Since the Government has yet to make any public declarations on even the existence of NETRA, information on particulars regarding the system or its operation is rather scanty. However, from the various recent news reports, it can be gathered that NETRA will essentially be a surveillance system designed specifically to monitor the nation's internet networks including voice traffic passing through software such as Skype or Google Talk, besides write-ups in tweets, status updates, emails, instant messaging transcripts, internet calls, blogs and forums.[50] Not much is known regarding how this is proposed to be done, what technology will be employed, under what authority it will operate or what procedural safeguards are in place to prevent misuse of intercepted data. NETRA being strictly an internet surveillance system, it should operate under the provisions Sections 69 and 69B of the Information Technology Act read with the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules and the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data and Information) Rules since they collectively prescribe the legal framework for interception of internet traffic and meta-data respectively. However, said legislations contain no provisions that allow the conduct of perpetual mass surveillance, which is exactly what NETRA seemingly does. So the question of how NETRA operates in conformance with governing laws as they stand today remains unanswered and open to speculation.

NETRA will essentially be a surveillance system designed specifically to monitor the nation's internet networks.

Various news reports have also stated that an inter-ministerial group comprising officials of the Cabinet Secretariat, Home Ministry, Defence Research and Development Organization, CAIR, Intelligence Bureau, Center for Develo-pment of Telematics and Computer Emergency Response Team that recently discussed the deployment strategy of NETRA favored allocation of 300 GB of storage space to a maximum of three security agencies, including the IB and Cabinet Secretariat, for intercepted internet traffic, with an extra 100 GB assigned to the remaining LEAs.[51] The resultant sum total of about 1 TB of storage for intercepted data would be a ridiculously minuscule amount. However, it was later clarified by an SFLC.in source with claimed direct links to the DRDO that NETRA storage servers known as 'nodes'

49 http://www.livemint.com/Politics/To4wvOZX7RmLM4VqtBshCM/India-to-deploy-Internet-spy-system-Netra.html accessed on February 12, 2014

50 Ibid.

51 http://articles.economictimes.indiatimes.com/2014-01-06/news/45918687_1_security-agencies-netra-inter-ministerial-group, accessed on February 12, 2014

will be installed at the ISP level at more than 1000 locations across India, each with a storage capacity of 300 GB. So a total of 300 TB of storage will be allocated initially. In any case, details surrounding the mysterious internet surveillance system continue to be hazy at best and one can only wait until more details emerge.

4.4 National Intelligence Grid

Conceptualized in the aftermath of the infamous 26/11 Mumbai terror attacks, NATGRID is envisioned as an ambitious counter-terrorism initiative to be undertaken on public-private partnership that will utilize technologies like Big Data and analytics to study and analyze huge amounts of data from various intelligence and enforcement agencies to help track suspects and prevent such attacks.[52]

> NATGRID will utilize technologies like Big Data and analytics to study and analyze huge amounts of data from various intelligence and enforcement agencies to help track suspects and prevent such attacks.

According to a response dated 9 June, 2011 from the NATGRID Office to an RTI request filed by SFLC.in, NATGRID will be established as an attached office of the Ministry of Home Affairs, as per the decision of the Cabinet Committee on Security (full text of NATGRID's response available at http://sflc.in/unravelling-natgrid/). It will reportedly collate and analyze data generated by 21 standalone databases belonging to various agencies and ministries of the Indian Government, which includes tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel.[53] It will then make this pool of data available to all security agencies — including the RAW, the IB, the ED, the National Investigation Agency, the CBI, the Directorate of Revenue Intelligence and the Narcotics Control Bureau.[54] Armed with the use of Big Data and other analytics technologies, NATGRID is also expected to facilitate robust information sharing by various LEAs, which will supposedly strengthen their ability to detect terrorist activity, and swiftly piece together information that could help pre-empt attacks or find the perpetrators in the unfortunate event.[55] To this end, in the budget of 2012-2013, the NATGRID was allotted funds to the tune of Rs. 364.80 crore, which was revised to just Rs. 10.99 crore due to non clearance for some of the plans by the Government. However, it witnessed a quantum jump in the 2013-2014 budget getting a six-fold increase with an allocation of Rs. 66.5 crore. The NATGRID is said to have been in partial operation since January 2013[56].[57]

52 http://www.business-standard.com/article/current-affairs/natgrid-to-use-big-data-analytics-to-track-suspects-113122900191_1.html, accessed on February 18, 2014
53 http://www.thehindu.com/news/national/article3529461.ece , accessed on February 18, 2014
54 Ibid.
55 http://pib.nic.in/newsite/erelease.aspx?relid=102034 , accessed on February 18, 2014
56 http://www.moneycontrol.com/news/current-affairs/natgrid-to-be-operational-by-jan-2013_555474.html , accessed on February 18, 2014
57 http://articles.economictimes.indiatimes.com/2013-12-22/news/45475848_1_natgrid-national-intelligence-grid-raman, accessed on February 18, 2014

Again, not much is known regarding the specifics of NATGRID, its governing laws or other procedural safeguards to prevent the leak or misuse of collated data that is clearly of a highly sensitive nature. Responding to the previously mentioned RTI request, the PMO further offered that all possible measures are being taken to prevent misuse of NATGRID, though the specific measures were refused to be disclosed 'for security reasons'. Interestingly, soon after a series of follow-up RTI requests , NATGRID was added to Schedule II of the RTI Act, which contains a list of Government instrumentalities excluded from the purview of the Act. Resultantly, concerned Public Information Officers are no longer obliged to entertain RTI requests relating to NATGRID and all subsequent requests have been categorically denied claiming this exemption.

In any case, NATGRID CEO Raghu Raman argues that rather than promoting invasion into people's privacy, NATGRID will protect all information and act as a deterrent to misuse of data, though the 'how' of it was left unaddressed. As per the initial plan, the user agencies will route their queries through NATGRID, which will function as a central facilitation centre, to data sources such as banks and airlines. These agencies will also get bolted-down computer terminals for accessing information from NATGRID.[58] However, bolted-down terminals are far from adequate protection against misuse of sensitive data and in the absence of any additional public statements on safeguard mechanisms within NATGRID, one is left at the all-too-familiar situation of depending on the user agencies' goodwill to prevent misuse of the sensitive personal data of citizens.

4.5 Unlawful interception and monitoring

Apart from the above-mentioned surveillance systems, whose existence at least are publicly known and whose operations may shakily be argued as legitimate in the eyes of law, there is reason to believe that the authorities also indulge in discreet communications surveillance practices, the legality of which are questionable at best. Please be mindful of the fact that this information is unverified .

For instance, SFLC.in was informed by a delegate at a recent conference that he manages a company that 'helps the Government track down terrorists'. What is truly disturbing about this ostensibly noble endeavour is the manner in which said 'terrorists' are tracked down. In the delegate's own words, his team of experts are given a list of individuals suspected of having links to terrorist organizations by various LEAs such as the CBI, based on which they proceed to infiltrate the targets' electronic communications including e-mail and chats through the use of trojans or other malicious software. Such software disguised as .jpg attachments among others, are injected into target systems by agents often assuming false identities that are determined to hold interest to the targets based on their age groups and other available

58 http://articles.economictimes.indiatimes.com/2011-06-12/news/29647514_1_natgrid-warsaw-data, accessed on February 18, 2014

information. Once the software is successfully injected, they proceed to secure access to personal data such as e-mail and IM IDs and passwords, which are used to log in to the corresponding user accounts and scan the contained communications histories for evidence of terrorist links. Any evidence so found is accordingly handed to the requisitioning LEAs that will then use said evidence in their own internal investigation processes. The delegate further indicated that his company is only one of several others engaged in a similar business model in India.

If true, the legality of operations of such private surveillance companies is entirely questionable in view of the fact that the Information Technology Act expressly criminalizes the infiltration and discreet retrieval of information of the nature discussed above. Additionally, the discreet nature of these endeavours means there is no public accountability or oversight involved whatsoever. This also brings up the rather unsettling question of what other discreet surveillance mechanisms are currently in deployment that we haven't had the fortune of coming to know of through chance encounters.

5. Privacy: The Indian Perspective

Having seen the many surveillance programs that keep a close watch on India's communication networks, one cannot help but ask the following question: what is the Indian take on a Right to Privacy?

On the outset, a Constitutional Right to Privacy is conspicuous only in its absence. However, this is not to say there hasn't been considerable debate in judicial and legislative circles on the matter.

> A seven-judge bench of the Supreme Court held that Article 21 of the Constitution of India contains an implicit right to privacy.

In the case of Kharak Singh v. The State of UP & Ors.[59], two judges of a seven-judge bench of the Supreme Court held that Article 21 of the Constitution of India, which guarantees citizens a Fundamental Right to Life and Personal Liberty, contains an implicit right to privacy. The same was held in Govind v. State of Madhya Pradesh[60] as well as R R Gopal & Anr. v. State of Tamil Nadu[61]. While the aforementioned cases examined a physical violation of privacy, in a more recent case of People's Union for Civil Liberties v. Union of India & Anr.[62], a two-judge bench of the Supreme Court examined the Constitutionality of Section 5(2) of the Indian Telegraph Act and came to the conclusion that the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as right to privacy. The judgement further said that telephone-tapping, unless conducted in accordance with procedure established by law, violates Articles 19(1)(a) and 21 of the Constitution. It also reiterated that while the right to privacy, by itself, has not been identified under the Constitution, it is still a part of the Right to Life and Personal Liberty enshrined under Article 21.

Thus, the judicial stand on the matter of privacy is clear, in that it recognizes right to privacy as an implicit content of Article 21, but admits that as a concept it may be too broad and moralistic to define judicially. Instead, the judiciary recommends that possible infringements of the right to privacy be examined on a case-by-case basis.

The citizens' privacy rights were once again brought under the judicial scanner in 2010, when the Supreme Court admitted a petition [*Ratan Tata v. UoI* {W.P.(C).No. 398 of 2010}] filed by renowned industrialist Ratan Tata, where Mr. Tata claimed that his right to privacy as guaranteed by Article 21 had been violated in view of the Government's failure to prevent the leakage and eventual publication of certain intercepted phone-conversations betwe-en himself and Niira Radia – a popular corporate lobbyist. He was aggrieved by the failure of the authorities to take

59 (1964) 1 SCR 332
60 (1975) 2 SCC 148
61 (1994) 6 SCC 632
62 (1997) 1 SCC 301

adequate steps to protect the privacy of those whose conversations were recorded, and to act in accordance with the Indian Telegraph Rules in dealing with these transcripts. In his petition, Mr. Tata sought directions from the Court to the effect that the authorities take all steps to retrieve the leaked recordings, and the CBI conduct a thorough inquiry into the matter. He also sought a direction to ensure that there was no further publication of these recordings. In light of the significant questions of law involved, the Supreme Court's decision in the matter is expected to significantly contribute to the existing judicial canon on right to privacy in the Indian context. Mr. Tata's petition is presently pending before the Court.

Aside from judicial pronouncements, right to privacy in India is also influenced by the Universal Declaration on Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR), both of which recognize the individual's right to privacy. While India is a signatory to the UDHR and ICCPR, provisions of these international documents are non-enforceable in law. However, it is almost an accepted proposition of law that the rules of customary international law which are not contrary to the municipal law shall be deemed to be incorporated in the domestic law. In addition, Article 51 of the Constitution directs that the State shall endeavour to *inter alia*, foster respect for international law and treaty obligations in the dealings of organised peoples with one another. Article 51 being a Directive Principle of State Policy, the contained direction is again non-enforceable. However, it serves as a constitutional reminder that the State's obligations under international law and treaties must not be transgressed. So in summation, India is under a non-enforceable obligation to incorporate Right to Privacy into its laws. Though non-enforceable, this obligation serves an important purpose of providing legally recognized ideals, the adoption of which every effort should be directed at. In other words, it serves as an accepted dictate that there needs to be a legislatively recognized Right to Privacy in India.

Further, a committee headed by Justice A P Shah published a report in October 2012, which dealt comprehensively with privacy laws across jurisdictions. The object of said report was to provide a set of recommendations on the right to privacy in light of expanding State and corporate surveillance capabilities in the digital age. The report identified nine National Privacy Principles that serve to establish safeguards and procedures over the collection, processing, storage, retention, access, disclosure, destruction, and anonymization of sensitive personal information, personal identifiable information, sharing, transfer, and identifiable information , along with the rights of the data subject in relation to such information:

1. *Notice at the time of collection of data, breach, access etc.*: At the time of collection, the content, use and purpose of collection must be notified to the data subject

2. *Choice and Consent*: The choice to (not) provide their personal

information must always be in the hands of the data subject

3. *Collection Limitation*: Only that data which is necessary for the object to be achieved must be sought from the data subject

4. *Purpose limitation*: The information must only be used for the purpose for which it is sought

5. *Access and Correction*: Data subjects should have access to their own information as well as the ability to correct and amend the information that is kept with the data controller

6. *Disclosure of Information*: The disclosure of personal information of the data subject shall only be given to third parties after their informed consent has been taken

7. *Security*: Reasonable security safeguards shall be put in place to ensure that unauthorized persons cannot access or destroy the data

8. *Openness*: Practices shall be implemented that ensure compliance with privacy principles

9. *Accountability*: The data controller shall be accountable for all the information that he keeps

The report aptly observes that currently, privacy protection in India is piecemeal and does not uphold these principles in a systematic function. Especially considering the entire array of surveillance systems that directly threaten the Right to Privacy of Indian citizens, an overarching Privacy Act, which specifically incorporates these principles and sets up an enforcement mechanism to ensure compliance is an immediate necessity.

While the privacy protection in India is inadequate in its current state, there have been significant dialogues in the international framework relating to a fundamental Right to Privacy in the online sphere. The next chapter accordingly looks beyond India and seeks to understand various internationally guaranteed human rights on which State surveillance would have significant bearing.

6. Surveillance and Human Rights

Articles 12 and 17 of the UDHR and ICCPR respectively guarantee a Right to Privacy.

Article 19 of both the UDHR[63] and the ICCPR[64] guarantee the people of the world a Right to Freedom of Opinion and Expression. These rights affirm that everyone has the right to hold opinions without interference, and to seek, receive and impart information and ideas of kinds through any media and regardless of frontiers. Unimpeded freedom of opinion and expression of the kind envisaged by the UDHR and ICCPR will be impossible if people must live in perpetual fear of sanction for their unpopular opinions or information, including those voiced in private fora.

Further, Articles 12 and 17 of the UDHR[65] and ICCPR[66] respectively guarantee a Right to Privacy. Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, and a private sphere with or without interaction with others, free from State intervention and excessive unsolicited intervention by other uninvited individuals.[67] However, the lack of explicit articulation of the content of this right has led to difficulties in its application and enforcement. There remain challenges with respect to what constitutes the private sphere and in establishing notions of what constitutes public interest.

General Comment No. 16 (1988) by the Center for Civil and Political Rights (CCPR), adopted by the Human Rights Council (HRC) of the United Nations (UN) said surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations, should be prohibited. It also indicated that the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. In its General Comment No. 34 (2011), the HRC analyzed the relationship

63 Article 19, UDHR: *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

64 Article 19, ICCPR: *1. Everyone shall have the right to hold opinions without interference.*
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart ideas and information of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

65 Article 12, UDHR: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

66 Article 17, ICCPR: *1. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.*
2. Everyone has the right to the protection of the law against such interference or attacks.

67 Lord Lester and D. Pannick (ed.), *Human Rights Law and Practice, 1st ed. 2004, para 4.82*

between the Right to Freedom of Expression and Opinion and the Right to Privacy, underlining how the latter is often an essential requirement for the realization of the latter.

Also relevant is the Resolution on Right to Privacy in the Digital Age[68] adopted by the UN General Assembly on 19th December 2013. The Resolution, jointly drafted by Germany and Brazil, has the U.N. General Assembly call upon its members 'to review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law'. It notes that new technologies that increase the ability for surveillance, interception and data collection by governments, companies and individuals may violate or abuse human rights, in particular the right to privacy. The adoption of this Resolution is a milestone since the General Assembly has established, for the first time, that human rights should prevail irrespective of the medium and therefore need to be protected both off-line and on-line.[69] While there has been much debate over the binding force of UN General Assembly Resolutions, they are generally accepted as legally non-binding. Nevertheless, the significance of the Resolution must not be undermined since it is indicative of the consensual point-of-view of an international consortium of nations on a matter of socio-legal significance. Though this might not strictly translate into immediate structural changes across the world, it undeniably has considerable import on international dialogues on the matter of state surveillance and human rights.

Further, the UN General Assembly had, in its above-mentioned Resolution on Right to Privacy in the Digital Age, asked the UN High Commissioner on Human Rights (HCHR) to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its 27th session and to the General Assembly at its 69th session. An advance copy of this Report was released by the office of the HCHR on 30th June 2014. With regard to surveillance and collection of personal data, the Report concludes that practices in many States reveal a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which contribute to a lack of accountability for arbitrary or unlawful interference in the right to privacy. As an immediate measure, the Report suggests that States review their own national laws, policies and practices to ensure full conformity with international human rights law. Where there are shortcomings, States should take steps to address them, including through the adoption of a clear, precise, accessible, comprehensive and non-discriminatory legislative framework. Steps should also be taken to ensure

68 A/RES/68/167

69 Statement made by the Representative of Brazil on adoption of the Draft Resolution on Right to Privacy in the Digital Age

that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy.

Thus the international policy sentiments towards unregulated surveillance conducted by States is clear in that there is a general consensus on the resultant violations of the Right to Privacy as well as the Right to Freedom of Expression and Opinion. Both the UN General Assembly's Resolution on Right to Privacy in the Digital age and the report of the HCHR on surveillance and collection of personal data emphasize this fact and call for immediate review of national laws followed by implementation of remedial measures.

7. The Necessary and Proportionate Principles

By now, it should be amply clear that Government authorities and Law Enforcement Agencies have near-unqualified surveillance capabilities when it comes to India's communication networks. Upcoming surveillance systems such as the CMS and NETRA are demonstrably among the most invasive in the world – all the more so, considering how a patchwork of broadly worded laws wallow them to tap into virtually any network, often without the knowledge of even service providers themselves. Additionally, the whole process has no parliamentary or judicial oversight whatsoever, and the conspicuous absence of a justiciable Right to Privacy in Indian legal canons makes matters even worse.

To further illustrate the undesirability of this state of affairs, we now turn to a set of 13 international principles[70] that seek to provide a frame of reference towards determining the fairness of State surveillance programs. Led by Privacy International, Access and Electronic Frontier Foundation, and ratified by hundreds of signatory organizations (including SFLC.in) from across the world, these principles are the outcome of a year-long global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology. Bearing in mind that privacy is a fundamental human right central to the maintenance of democratic societies, the principles also serve as a comprehensive explanation of how existing human rights standards and international law apply to the new capabilities and risks of digital surveillance.

Without further ado, the determination of whether the State may conduct communications surveillance that interferes with protected information must be consistent with the following principles:

7.1 Legality

"*Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the Right to Privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the Right to Privacy should be subject to periodic review by means of a participatory legislative or regulatory process.*"

Central/State Governments, their authorized agents and LEAs in India derive their authority to conduct communications surveillance from several legislative Acts and Rules in addition to the collective body of communications service licenses, as seen in chapters II and III. These include the Indian Telegraph Act 1885, Information Technology Act 2000, Rules framed under these Acts, Code of Criminal Procedure 1973 and service licenses granted by the Department of Telecommunications to communications service providers – including but not limited to the Unified Access Service

70 Available at https://en.necessaryandproportionate.org/text

License, Internet Service License and Unified License. Thus, measures that limit citizens' Right to Privacy arguably have their foundations in publicly available legislations and regulations.

However, there is a deeper underlying problem here in that citizens of India do not enjoy a justiciable and legislatively granted Right to Privacy to begin with. Right to Privacy in India is an uncertain, non-justiciable right that exists solely on the basis of its judicial interpretation as an implicit content of Right to Life as guaranteed by Article 21 of the Constitution of India.

Further, most surveillance-enabling laws and regulations rarely, if ever, see review in order to keep up with technological changes. For instance, provisions dealing with interception/monitoring of telephones are found under the archaic Indian Telegraph Act of 1885. Its provisions have also served as the bases for more recent additions such as Section 69 to the Information Technology Act, which was modelled after Section 5 of the Telegraph Act. In this particular instance, much of the language of law has been retained over the two Acts that are separated by over a century. So specific provisions contained in the enabling legislations do not reflect recent advancements in technology, leading to a significant amount of administrative difficulties to the detriment of all involved.

7.2 Legitimate aim

"*Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.*"

The crux of the principle of legitimate aim is that communications surveillance should be undertaken only towards achieving a 'predominantly important legal interest that is necessary in a democratic society'. This rightly narrows down the scope of invasive surveillance mechanisms to the most dire circumstances, where the very foundations of democratic society are at stake. With the bar set so high, surveillance cannot be undertaken on shaky grounds and in the interest of trifling ends.

An examination of the surveillance-enabling provisions found across Indian legislations will reveal that communications surveillance is currently permitted on a wide variety of broadly worded grounds, and this includes everything from protection of national security to prevention of spread of computer viruses. These validating grounds cover a ridiculous number of situations and have such sweeping ambit that legitimacy of aim is all but lost, since they effectively allow unrestricted communications surveillance to be conducted on anyone at any time.

The principle of legitimate aim therefore does not find compliance in India's communications surveillance regime.

7.3 Necessity

"*Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.*"

Drawing upon the preceding principle, the principle of necessity states that communications surveillance may be conducted only when it is the least intrusive means of attaining the legitimate aim. Once again, the threshold of justifiability of surveillance is rightly set very high

Strictly speaking, Rule 419A(3) of the Indian Telegraph Rules 1951 and Rule 8 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 do stipulate that 'other reasonable means' must be considered and exhausted before issuing an interception or monitoring order under the Rules. However, these cautionary provisions are purely procedural hurdles to the actual retrieval of intercepted information. Considering that around 7500 - 9000 phone-interception orders were issued by the Central Government every month (as revealed by an RTI request filed by SFLC.in), careful consideration of less intrusive alternatives in each case would be physically impossible. Further, surveillance systems such as NETRA, which *perpetually* monitor communication networks call into question the whole premise of Rules 419A and 8, since continuous availability of intercepted data would have the effect of dispensing with the very need to resort to other less intrusive means. Also, in the absence of independent oversight, there is no obligation to justify this choice of means. Thus, despite compliant legislative provisions, the principle of necessity sees questionable compliance at best in the bigger picture.

7.4 Adequacy

"*Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.*"

The principle of adequacy states that the choice of specific means of communications surveillance must correspond to the legitimate aim at hand. In other words, the mere existence of a legitimate aim must not be grounds for indulging in all kinds of communications surveillance, but the best suited form of surveillance must be identified and employed based on the surrounding circumstances.

However, as already seen, communications surveillance in India is not always conducted in pursuance of a legitimate aim for want of less intrusive alternatives. The nation's communication networks are effectively under perpetual surveillance, with the retrieval of collected information being conditional on the LEAs' procurement of a lawful order to do so. Also considering the sheer volume of such lawful orders issued, a case-by-case determination of whether surveillance is

the best alternative under the circumstances is almost certainly never done. In the face of such perpetual and unrestricted surveillance, compliance with the principles of legality, necessity or adequacy looks uncertain.

7.5 Proportionality

"*Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.*

Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

> *• There is a high degree of probability that a serious crime has been or will be committed;*
>
> *• Evidence of such a crime would be obtained by accessing the protected information sought;*
>
> *• Other available less invasive investigative techniques have been exhausted;*
>
> *• Information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and*
>
> *• Information is accessed only by the specified authority and used for the purpose for which authorization was given.*

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

> *• Other available less invasive investigative techniques have been considered;*
>
> *• Information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and*
>
> *• Information is accessed only by the specified authority and used for the purpose for which was authorization was given.*"

This principle essentially states that the benefits of communications surveillance should always outweigh its costs i.e. surveillance should be only be resorted to following extensive contemplation of the benefits sought to be derived in contrast with the costs associated in the form of compromise of privacy. As much should

also be demonstrated before a competent, independent and impartial authority and only once this is done should the actual surveillance commence.

As already explained, this is hardly the currently practised model of communications surveillance in India. Surveillance is allowed for a number of broadly worded grounds, several of which do not qualify as legitimate aims, there isn't sufficient weighing of benefits against costs and there is no requirement to demonstrate the necessity of conducting surveillance before a judicial authority. Further, certain surveillance systems such as NETRA seemingly conduct *perpetual mass surveillance*, affording no opportunities for cost-benefit-analyses in specific instances. It would appear that communications surveillance is mostly undertaken because it is the easiest available alternative, as opposed to the least intrusive.

7.6 Competent judicial authority

"*Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:*

> 1. *Separate from the authorities conducting communications surveillance;*
>
> 2. *Conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and*
>
> 3. *Have adequate resources in exercising the functions assigned to them.*"

This principle is *prima facie* violated by India's communications surveillance framework for the simple reason that there is absolutely no judicial intervention at any stage of the surveillance process. No provisions of law as they currently stand talk about judicial oversight in any capacity. An observation on the matter was also made by the Supreme Court in the case of PUCL v. UoI,[71] where judicial oversight of phone interception was held as unsustainable in the lack of express legal provisions that provide for such oversight.

Though the Indian Telegraph Rules and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules provide for the establishment of a Review Committee towards reviewing surveillance directives, this Committee is comprised solely of members of the executive. When provisions of law stipulate systematic review of any activity capable of causing harm in the absence of oversight, it logically follows that fairness of review cannot be guaranteed in the presence of conflicting interests. If those undertaking and reviewing such potentially harmful activity belong to the same broad vehicle of the Government, conflicting interests are all but unavoidable and this leads to a complete breakdown of the review process itself.

As per the governing Acts and Rules, an order authorizing communications surveillance may be issued by the

71 (1997) 1 SCC 301

'competent authority' i.e. the Secretary in the Ministry of Home Affairs/Secretary in charge of the Home Department; actual surveillance is carried out mostly by authorized LEAs; and the Review Committee consists of the Cabinet/Chief Secretary along with Secretaries in charge of legal affairs and telecommunications. In other words, every aspect of India's surveillance regime is handled by the executive arm of the Government with no judicial intervention whatsoever and therefore, just and fair review of surveillance process is nearly impossible. Thus, the principle of competent judicial authority stands violated in its entirety.

7.7 Due process

"*Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law, except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorization must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorization.*"

As previously mentioned, Indian communications surveillance is technically founded in publicly available law. However, there are no means of determining the extent to and rigor with which these laws are observed in practice, since all of India's communications surveillance is conducted within an extremely closed environment with no transparency or independent oversight. The concerned enabling Acts and Rules always stipulate the observance of strict confidentiality in the surveillance process, thereby significantly limiting the amount of information on surveillance practices that is available to the general public. Government authorities routinely assure citizens that surveillance is conducted only in accordance with law, yet this claim is questionable. For instance, despite consistent assurances that the CMS operates strictly in accordance with the procedures laid down by Rule 419A of the Indian Telegraph Rules, its capability for Direct Electronic Provisioning, i.e. automated instantaneous interception without involvement of service providers, runs foul of this procedure. Similarly, there are no provisions of law that provide for the conduct of mass surveillance of any kind, yet exactly this what NETRA seemingly does when it scans the nation's internet traffic for trigger words and phrases.

Thus while publicly available law does enumerate procedures that govern interference with human rights, its consistent practice remains questionable. And even though legal remedies are available with respect to violation of rights, the efficacy of these remedies is somewhat compromised in the face of emphatic claims of legal compliance accompanied by the inability to verify these claims.

7.8 User notification

"*Individuals should be notified of a decision authorizing communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorization. Delay in notification is only justified in the following circumstances:*

> 1. *Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; or*
>
> 2. *Authorization to delay notification is granted by the competent judicial authority at the time that authorization for surveillance is granted; and*
>
> 3. *The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.*"

There currently exist no provisions of law whereby users are notified when their communications are subjected to surveillance, and no distinction is made between situations where such notification would defeat the purpose of surveillance and otherwise. By extension, users also lack the ability to appeal the decision to surveille their communications. Even once active surveillance has been concluded, collected information is retained for specified periods after which they are destroyed – all without intimating the user. Thus it is entirely possible in the present scenario for the bulk of a users' communications to be subjected to extensive surveillance leaving him/her none the wiser.

7.9 Transparency

"*States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.*"

The principle of transparency is *prima facie* violated by Indian communications surveillance. Government authorities and LEAs view communications surveillance as an exclusive State concern in which non-governmental parties have no business interfering. This is evident in the fact that surveillance systems such as the CMS and NETRA are sanctioned by high-level ministerial committees without

adequate parliamentary dialogue. The CMS in particular, while commencing initial operations, had only a partial in-principle approval from the Cabinet Committee on Security. Even questions raised by Members of Parliament on such matters are answered in such a way that as little information is divulged as possible. Save a few rare press releases, little to no information is publicly shared regarding surveillance initiatives and even purely procedural information such as internal guidelines requested under the Right to Information Act is consistently denied claiming exemption under Section 8(1)(a) as they relate to national security matters. With most of the information on State surveillance initiatives coming from investigative reports by various non-state parties, the resulting picture is a patchwork of verified data, unverified rumors and wild speculations, all of which significantly contribute to the confusion surrounding India's communications surveillance regime.

7.10 Public oversight

"*States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.*"

Once again, all oversight of Indian communications surveillance is carried out by a single Review Committee constituted under Rule 419A of the Indian Telegraph Rules, which comprises entirely of members of the executive. This severely compromises its independence and impartiality due to the apparent conflict of interest that arises when the authorization, conduct and review of communications surveillance is carried out by a singular arm of the Government machinery. Additionally, the Committee's scope of review is restricted to the sustainability of specific interception directives issued by the concerned authorities, and does not extend to the mode of interception or subsequent use of intercepted information.

Thus the only oversight of Indian communications surveillance is of an executive nature, and has very limited scope. The public oversight principle is therefore not complied with.

7.11 Integrity of communications and systems

"*In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular*

information purely for State surveillance purposes. A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision."

Thus the fundamental concern of this principle is the security of communication networks and systems. Towards securing said networks and systems, it is recommended that:

- There should be no compulsion on vendors/service providers to facilitate surveillance

- User identification must not be a precondition for service provision

Regarding the facilitation of surveillance, service licenses place Indian communications service providers under the express obligation to install surveillance equipment into their networks as and when required by the Government 'in the interest of security'. Apart from the threat of license revocation on failure to comply, surveillance-enabling provisions of law such as those found under the Indian Telegraph Act or Information Technology Act further strengthen this compulsion by prescribing penalties on the failure to provide information when called upon to do so. In addition, service providers are prohibited by service licenses from employing bulk encryption in their networks, and even when non-bulk, anything higher than a 40-bit encryption requires express approval from the Department of Telecommunications. This ban on encryption beyond 40-bits extends to individuals, groups and organizations as well. All these undeniably compromise the general security of communications networks by facilitating not only surveillance initiatives, but also malicious and targeted attacks from non-state parties.

Further, user identification is always a prerequisite for provision of communications service. Citizens are required to provide valid identification when procuring new telephone or internet connections and even when using cyber cafes for internet access. Communications service providers are also required to maintain regularly updated lists of all subscribers and make them available to authorized Government agencies. This indicates that the Government is intolerant of anonymity in the telecommunication or internet circles, and wish to be able to trace specific instances of communication to their respective points of origin.

In short, the above measures have the cumulative effect of doing exactly what the principle of integrity seeks to avoid i.e. compromising the general security of communications, as well as disallowing user anonymity in all communication spheres.

7.12 Safeguards for international cooperation

"*In response to changes in the flows of*

information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLAT) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness."

This principle essentially says that MLATs and other international agreements should not present opportunities to conduct invasive communications surveillance that would normally be disallowed in the domestic context. India currently has subsisting MLATs with 35 nations including USA, UK, Canada, France and Russia, but there are no explicit references to communications surveillance in any of said MLATs. Instead, they contain provisions that allow the request of information and evidence, surrounding which strict confidentiality must be maintained and measures implemented to prevent unauthorized access or misuse. However, this does not provide for the application of highest available standards of individual protection since there is no weighing of options involved. MLATs and other international agreements as they currently stand do not deal with communications surveillance in sufficient detail and hence the intricacies involved in international cooperation in the realm of communications surveillance still need to be worked out.

7.13 Safeguards against illegitimate access

"*States should enact legislation criminalizing illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.*"

The following provisions of law deal with unauthorized access of communications:

- Section 24 read with Section 23 of the Indian Telegraph Act punishes any person, who attempts to unlawfully learn the contents of communications, with imprisonment up to one year and fine up to Rs. 500. However, the circumstances inviting penalty are limited in scope as they require the offender to physically enter Government premises or obstruct Government officials while attempting to unlawfully learn the

contents of communications.

• Section 26 of the Indian Telegraph Act punishes Government officials, who intercept, detain or disclose the content of communications without authorization, with imprisonment up to three years and fine.

• Section 43 of the Information Technology Act states that any person, who accesses and tampers with electronic devices, their content, or networks without authorization from their owner/person-in-charge, is liable to compensate the owner/person-in-charge for damages up to Rs. 1 crore.

• Section 72 of the Information Technology Act punishes any person, who discloses information that was lawfully accessed by him/her, with imprisonment up to two years and fine up to Rs. 2 lakhs.
The above provisions of law visibly penalize illegitimate communications surveillance by both public and private actors. Also, both the Indian Telegraph Act and the Information Technology Act stipulate the destruction of all surveillance- related documents within specified periods once active surveillance has been concluded.

However, since a majority of these collective principles are not conformed to in Indian conduct of communications surveillance to begin with, the inadmissibility of information collected through non-conformant surveillance as evidence does not arise. Nor does the law tackle the admissibility of information collected in violation of its own mandates. Thus, the principle of safeguards against illegitimate access can be considered only partially observed in India.

In summation, it is seen that Indian communications surveillance is conducted in violation of most of the international principles discussed in this chapter. The principles of legitimate aim, proportionality, competent judicial authority, user notification, transparency, public oversight, and integrity of communications and systems stand entirely violated. Even the remaining principles i.e. legality, necessity and due process see only partial/questionable compliance. This clearly indicates that Indian communications surveillance is conducted in a manner that is far from what may be considered just . Of the discussed contraventions of principles, lack of a legislatively granted Right to Privacy, lack of judicial oversight and lack of transparency in surveillance require immediate and undivided attention from the law-makers since these shortcomings have the potential to translate into significant damage to the citizens of India, all the more so in the face of intrusive surveillance systems that are steadily escalating in their scale of operations.

8. Conclusion

Over the course of this report, we have seen that the GoI and its agents are authorized under various statutes and license agreements to surveil India's telephone and Internet networks on a large number of broadly worded grounds ranging from protection of national security to preventing the spread of computer viruses. Pursuant to authority so derived, several state surveillance programs already keep a close tab on our communication networks, and far more potent surveillance technologies are in the pipeline in varying stages of deployment. While the Government swears that it limits itself to targeted surveillance and does not indulge in mass surveillance of any kind, the large scale data-mining and profiling capabilities of upcoming surveillance systems such as the CMS and NATGRID are reason enough to be skeptical of this stance. Also causing concern among citizens is the fact that communications surveillance continues to be the exclusive domain of the Executive arm of the Government, which insists on keeping the public in the dark. There are no provisions for public or judicial oversight of the surveillance process and in such a scenario, one cannot help but be wary of abuse of power. To top it all off, a legislatively recognized right to privacy is conspicuously absent from Indian legal canons. Protection accorded by law to the citizens' right to privacy ends with a judicial interpretation of the right as an implicit content of right to life as guaranteed by the Constitution of India.

In the wake of the global uproar caused by Edward Snowden's revelations on US surveillance, and the sudden spike in interest around the topic of surveillance and privacy, the time has come for a comprehensive review of Indian legislative provisions that sanction and regulate our surveillance process. In this regard, the language of the law needs to be considerably narrowed down to specify objectively verifiable situations under which surveillance may be legitimately undertaken. The procedure to be followed while surveilling communications must be clearly spelled out in its entirety, and any opportunity for misuse of authority must be done away with by holding the concerned agents of intercepting agencies to the highest standards of accountability. Provision for independent oversight of the surveillance process is an immediate necessity, and the regime of blanket denial of surveillance-related information requests made by the public must be done away with. The surveillance regime in its current state needs to be made more transparent, and public trust in this regard must be rebuilt, which will not happen without a greater degree of public participation. Finally, citizens must have a legislatively recognized right to privacy, the violation of which will entitle them to constitutional remedies.

All of the above remedies are easily envisioned, but their implementation will undoubtedly present several challenges – both foreseen and unforeseen. Nothing short of a collective, concentrated effort on the part of all stakeholders in the surveillance regime, including but not limited to the Government, industry, civil society and the general public, will serve to transform India's surveillance state from its current state of opacity to one of transparency, trust and efficiency.

Appendix

The Information Technology Act, 2000

Section 28 - Power to investigate contraventions.

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.
(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

Section 29 - Access to computers and data.

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person in-charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

Section 43 - Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, —

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to

any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.
Explanation.—For the purposes of this section,—

(i) "computer contaminant" means any set of computer instructions that are designed—

> (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
>
> (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a progr-amme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Section 69 – Power to issue directions for interception or monitoring or decryption of any information through any computer resource

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing the incitement to the commission of any cognizable offence relating to the above or for the investigation of any offence, it may, subject to the provisions of sub-section

(2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be

intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to -

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be, or;

(c) provide information stored in computer resource

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

Section 69B - Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,

(i) "Computer Contaminant" shall have the meaning assigned to it in section 43

(ii) "traffic data" means any data identifying or purporting to identify any person, computer

system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Section 72 - Penalty for breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Indian Telegraph Act, 1885

Section 5 - Power for Government to take possession of licensed telegraphs and to order interception of messages

(1) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.

(2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:

Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section.

Section 3(1AA) - Definitions

'telegraph' means any appliance, instrument, material or apparatus used pr 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 Herizan waves, galvanic, electronic or magnetic means.

Explanation- 'Radio waves' or 'hertizan waves' means electro- magnetic waves of frequencies lower than 3,000 giga-cycles per second propagated in space without artificial guide.

Section 23 - Intrusion into signal-room, trespass in telegraph office or obstruction

If any person--

a) without permission of competent authority, enters a signal-room of a telegraph office of the Government, or of a person licensed under this Act, or

b) enters a fenced enclosure round such a telegraph office in contravention of any rule or notice not to do so, or

c) refuses to quit such room or enclosure on being requested to do so by any officer or servant employed therein, or

d) wilfully obstructs or impedes any such officer or servant in the performance of his duty, he shall be punished with fine which may extend to five hundred rupees.

Section 24 - Unlawfully attempting to learn the contents of messages

If any person does any of the acts mentioned in Section 23 with the intention of unlawfully learning the contents of any message, or of committing any offence punishable under this Act, he may (in addition to the fine with which he is punishable under Section 23) be punished with imprisonment for a term which may extend to one year.

Section 26 - Telegraph officer or other official making away with or altering, or unlawfully intercepting or disclosing messages, or divulging purport of signals.

If any telegraph officer, or any person, not being a telegraph officer, but having official duties connected with any office which is used as a telegraph office—

(a) wilfully, secrets, makes away with or alters any message which he has received for transmission or delivery, or

(b) wilfully, and otherwise than in obedience to an order of the Central Government or of a State Government, or of an officer specially authorised [by the Central or a State Government] to make the order, omits to transmit, or intercepts or detains, any message or any part thereof, or otherwise than in pursuance of his official duty or in obedience to the direction of a competent Court, discloses the contents or any part of the contents of any message, to any person not entitled to receive the same, or

(c) divulges the purport of any telegraphic signal to any person not entitled to become acquainted with the same,he shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.

Indian Telegraph Rules, 1951

Rule 419-A

(1) Directions for interception of any message or class of messages under sub-section (2) of Section 5 of the Indian Telegraph Act, 1885 shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government. In unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorized by the Union Home Secretary or the State Home Secretary, as the case may be:
Provided that in emergent cases—

> (i) in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or
>
> (ii) for operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible;

the required interception of any message or class of messages shall be carried out with the prior approval of the Head or the second senior most officer of the authorized security *i.e.* Law Enforcement Agency at the Central Level and the officers authorised in this behalf, not below the rank of Inspector General of Police at the state level but the concerned competent authority shall be informed of such interceptions by the approving authority within three working days and that such interceptions shall be got confirmed by the concerned competent authority within a period of seven working days. If the confirmation from the competent authority is not received within the stipulated seven days, such interception shall cease and the same message or class of messages shall not be intercepted thereafter without the prior approval of the Union Home Secretary or the State Home Secretary, as the case may be.

(2) Any order issued by the competent authority under sub-rule (1) shall contain reasons for such direction and a copy of such order shall be forwarded to the concerned Review Committee within a period of seven working days.

(3) While issuing directions under sub-rule (1) the officer shall consider possibility of acquiring the necessary information by other means and the directions under sub-rule (1) shall be issued only when it is not possible to acquire the information by any other reasonable means.

(4) The interception directed shall be the interception of any message or class of messages as are sent to or from any person or class of persons or relating to any particular subject whether such message or class of messages are received with one or more addresses, specified in the order, being an address or addresses likely to be used for the transmission of communications from or to one particular person specified or described in the order or one particular set of premises specified or described in the order.

(5) The directions shall specify the name and designation of the officer or the authority to whom the intercepted message or class of messages is to be disclosed and also specify that the use of intercepted message or class of messages shall be subject to the provisions of sub-section (2) of Section 5 of the said Act.

(6) The directions for interception shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of issue and may be renewed but the same shall not remain in force beyond a total period of one hundred and eighty days.

(7) The directions for interception issued under sub-rule (1) shall be conveyed to the designated officers of the licensee(s) who have been granted licenses under Section 4 of the said Act, in writing by an officer not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank.

(8) The officer authorized to intercept any message or class of message shall maintain proper records mentioning therein, the intercepted message or class of messages, the particulars of persons whose message has been intercepted, the name and other particulars of the officer or the authority to whom the intercepted message or class of messages has been disclosed, the number of copies of the intercepted message or class of messages made and the mode or the method by which such copies are made, the date of destruction of the copies and the duration within which the directions remain in force.

(9) All the requisitioning security agencies shall designate one or more nodal officers not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank to authenticate and send the requisitions for interception to the designated officers of the concerned service providers to be delivered by an officer not below the rank of Sub-lnspector of Police.

(10) The service providers shall designate two senior executives of the company in every licensed service area/State/Union Territory as the nodal officers to receive and handle such requisitions for interception.

(11) The designated nodal officers of the service providers shall issue acknowledgment letters to the concerned security and Law Enforcement Agency within two hours on receipt of intimations for interception.

(12) The system of designated nodal officers for communicating and receiving the requisitions for interceptions shall also be followed in emergent cases/ unavoidable cases where prior approval of the competent authority has not been obtained.

(13) The designated nodal officers of the service providers shall forward every fifteen days a list of interception authorizations received by them during the preceding fortnight to the nodal officers of the security and Law Enforcement Agencies for confirmation of the authenticity of such authorizations. The list should include details such as the reference and date of orders of the Union Home Secretary or State Home Secretary,

date and time of receipt of such orders and the date and time of Implementation of such orders.

(14) The service providers shall put in place adequate and effective internal checks to ensure that unauthorized interception of messages does not take place and extreme secrecy is maintained and utmost care and precaution is taken in the matter of interception of messages as it affects privacy of citizens and also that this matter is handled only by the designated nodal officers of the company.

(15) The service providers are responsible for actions for their employees also. In case of established violation of license conditions pertaining to maintenance of secrecy and confidentiality of information and unauthorized interception of communication, action shall be taken against the service providers as per Sections 20, 20-A, 23 & 24 of the said Act, and this shall include not only fine but also suspension or revocation of their licenses.

(16) The Central Government and the State Government, as the case may be, shall constitute a Review Committee. The Review Committee to be constituted by the Central Government shall consist of the following, namely:

(a) Cabinet Secretary.—Chairman

(b) Secretary to the Government of India Incharge, Legal Affairs—Member

(c) Secretary to the Government of India, Department of Telecommunications—Member

The Review Committee to be constituted by a State Government shall consist of the following, namely:

(a) Chief Secretary— Chairman

(b) Secretary Law/Legal Remembrancer Incharge, Legal Affairs — Member

(c) Secretary to the State Government (other than the Home Secretary)— Member

(17) The Review Committee shall meet at least once in two months and record its findings whether the directions issued under sub-rule (1) are in accordance with the provisions of sub-section (2) of Section 5 of the said Act. When the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above it may set aside the directions and orders for destruction of the copies of the intercepted message or class of messages.

(18) Records pertaining to such directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and the authorized security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements.

(19) The service providers shall destroy records pertaining to directions for interception of message within two months of discontinuance of the interception of such messages and in doing so they shall maintain extreme secrecy.

The Information Technology (Intermediaries Guidelines) Rules, 2011

Rule 3(7) - Due diligence to be observed by intermediary

When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Rule 6-Disclosure of information.

(1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:

Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

Information Technology (Guidelines for Cyber Cafe) Rules, 2011

Rule 7 - Inspection of Cyber Cafe

(1) An officer, not below the rank of Police Inspector as authorised by the licensing agency, is authorized to check or inspect cyber café and the computer resource or network established therein at any time for the compliance of these rules. The cyber café owner shall provide every related document, registers and any necessary information to the inspecting officer on demand.

Code of Criminal Procedure

Section 91 - Summons to produce document or other thing.

(1) Whenever any Court or any officer in charge of a police station considers that the production of any document or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a written order, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.

(2) Any person required under this section merely to produce a document or other thing shall be deemed to have complied with the requisition if he causes such document or thing to be produced instead of attending personally to produce the same.

(3) Nothing in this section shall be deemed -

(a) to affect, sections 123 and 124 of the Indian Evidence Act, 1872 (1 of 1872), or the Bankers, Books Evidence Act, 1891(13 of 1891), or

(b) to apply to a letter, postcard, telegram or other document or any parcel or thing in the custody of the postal or telegraph authority.

Notes

sflc.in

ABOUT SFLC.IN

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.

K-9, Birbal Road, Second Floor,
Jangpura Extension
New Delhi-110014, India
Tel: +91-11-43587126
Fax: +91-11-24320809
www.sflc.in

WORLD WIDE WEB FOUNDATION

With support from

World Wide Web Foundation's Web We Want Initiative

The World Wide Web Foundation was established in 2009 by Web inventor Sir Tim Berners-Lee to tackle the fundamental obstacles to realizing his vision of an open Web available, usable, and valuable for everyone. Their global initiative "Web We Want " is a global movement to defend, claim and change the future of the Web. The campaign is responding to threats to the future of the Web with a practical and positive vision — unleashing the power of people from around the world to defend, claim and change a Web that is for everyone. We aim to bring about real change at a national and global level. "

INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES) RULES, 2011

AN ANALYSIS

Defender of Your Digital Freedom!

Table of Contents

List of Abbreviations ..... *i*
List of Cases ..... *ii*
List of Statutes ..... *iii*
1. Introduction 1
    1.1 Methodology 2
2. Provisions of Information Technology Act, 2000 related to Intermediaries 4
    2.1 Definition of Intermediary 5
    2.2 Safe Harbour under Section 79 of the Act 7
3. Analysis of the Intermediaries Guidelines Rules 8
    3.1 Procedure for take-down of user generated content 8
    3.2 The Rules - Opinions of users and businesses 10
        3.2.1 Uncertainty regarding prohibited content 10
        3.2.2 Rights of content-creators 11
        3.2.3 Adjudicatory role to intermediaries 11
        3.2.4 Operational difficulty for Industry 12
        3.2.5 Privacy of users 12
    3.3 Differentiating private take-down from the government's powers for blocking access 13
    3.4 Need for a private take-down mechanism 13
    3.5 Legal analysis of the Rules 14
        3.5.1 Sub-rule (2) of Rule 3 14
        3.5.2 Sub-rule (4) of Rule 3 15
        3.5.3 Sub-rule (5) of Rule 3 17
        3.5.4 Sub-rule (7) of Rule 3 18
    3.6 Safe-harbour and Take-down mechanism in the Copyright Act 19
    3.7 Comparison of legislations in other countries on Intermediary Liability 19
        3.7.1 United Kingdom 19
        3.7.2 The United States of America 21
        3.7.3 Australia 22
        3.7.4 Brazil 24
        3.7.5 Summary of take-down provisions in countries 25
4.Recommendations of the Lok Sabha Committee on Subordinate Legislation 26
5. Motion to annul Information Technology (Intermediaries Guidelines) Rules, 2011 29
6. Reports and studies 32
    6.1 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression 32
    6.2 Study on Indian Online Intermediaries and the Liability System 33
    6.3 Policy brief on Intermediary Liability developed by Article 19 34
7. Feedback from Round-table discussions 35
8. Principles for a take-down system 39
9. Conclusion 40
Annexure 1 - The Information Technology (Intermediaries guidelines) Rules, 2011 41
Annexure 2 - Draft Rules circulated by SFLC.IN during the Round-table consultations 44

LIST OF ABBREVIATIONS

ACMA	Australian Communications and Media Authority
Cr.PC	Code of Criminal Procedure
CRAC	Cyber Regulation Advisory Committee
DEITy	Department of Electronics and Information Technology
EU	European Union
IAMAI	Internet and Mobile Association of India
ISP	Internet Service Provider
IWF	Internet Watch Foundation
MCIT	Ministry of Communications and Information Technology
OSP	Online Service Providers
PUCL	People's Union for Civil Liberties
TRAI	Telecom Regulatory Authority of India

LIST OF CASES

- *Express Newspapers (Private) Ltd. & Anr. v. The Union of India & Ors.* AIR 1958 SC 578
- *Gobind v. State of Madhya Pradesh* (1975) 2 SCC 148
- *Nirmaljit Singh Narula v. Indijobs at hubpages.com & Ors.* 190 (2012) DLT 51
- *People's Union for Civil Liberties v. Union of India & Anr.* (1997)1 SCC 301
- *R. Raj Gopal v. State of Tamil Nadu* (1994) 6 SCC 632
- *Rajeev Chandrasekhar v. Union of India* (Supreme Court) *W.P.(C) No. 23 of 2013*
- *Shreya Singhal v. Union of India* (Supreme Court) *W.P(Crl) 167/2012*
- *Tata Press Ltd. v. Mahanagar Telephone Nigam Limited and Ors* (1995) 5 SCC 139
- *The Secretary, Ministry of Information & Broadcasting v. Cricket Association Of Bengal* 1995 AIR SC 1236
- *Yahoo India Pvt. Ltd. v. Union of India & Another* (High Court of Delhi) W.P.(C).No. 6654/2011

LIST OF STATUTES

National Laws:

- The Information Technology Act, 2000
- The Information Technology (Amendment) Act, 2008
- The Information Technology (Intermediaries Guidelines) Rules, 2011
- The Information Technology (Procedures and Safeguards for Interception, Monitoring and
- Decryption of Information) Rules, 2009
- The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
- The Copyright (Amendment) Act, 2012
- The Copyright Rules, 2013

Laws in other jurisdictions:

- The Digital Millennium Copyright Act (US)
- The Communications Decency Act (US)
- The Trademark Act, 1946 (US)
- The EC Directive, 2000/31/EC (EU)
- The Electronic Commerce (EC Directive) Regulations, 2002 (UK)
- The Defamation Act, 2013 (UK)
- The Defamation (Operators of Websites) Regulations, 2013 (UK)
- The Copyright Act, 1968 (Australia)
- The Copyright Regulations, 1969 (Australia)
- The Broadcasting Services Amendment (Online Services) Act, 1999 (Australia)
- The Broadcasting Services Act, 1992 (Australia)
- National Classification Code, (May 2005) (Australia)
- Marco Civil da Internet (Brazil)

1. Introduction

As the Internet penetration in India grows, the medium offers great potential for information exchange, services delivery as well as political discourse. Various platforms like Facebook, Twitter and blogs make it easy for people to communicate and to get their messages across a vast audience. The potential for content to be delivered in local languages makes the medium more accessible to the common man all over the country.

> ***Regulation of content is often carried out by pressurising the intermediaries who provide services to users enabling them to post online content and communicate with each other***

According to the Indian Telecom Services Performance Indicators Report released by TRAI[1] on April 28, 2014, the total number of Internet subscribers in India at the end of December 2013 is 238.71 million. This growth is largely fuelled by the increasing mobile penetration with subscribers who accessed Internet through mobile devices constituting 219.92 million. A study conducted by the Internet and Mobile Association of India(IAMAI) predicted that in 160 constituencies, Facebook would be a critical tool that could influence the results in the 2014 Lok Sabha elections[2]. With increasing penetration and the growth of mobile, Internet has become a tool for expressing oneself and to voice views and opinions. The importance of social media as a tool for people mobilisation and to influence opinion formation was visible during the campaign against corruption launched by Anna Hazare, the outpour demanding justice for the December 16 rape victim, "Nirbhaya" or the Section 377 judgment by the Supreme Court of India. Anything that has such a wide ranging impact on different parts of our ecology presents immense opportunities along with challenges. Social media has changed the rules of the game by moving into a domain which was not very long ago restricted to either nationalised platforms or corporate owned spaces.

Governments are often compelled to regulate the flow of information and communication in this medium for a variety of reasons. Such regulation is often carried out by pressurising the intermediaries who provide services to users enabling them to post online content and communicate with each other. This is so because intermediaries, inter alia, act as "middle-men" providing platforms to the users, are easy to identify and impose "responsibility" on, and may be able to provide the identification information of users. The issue often debated is the liability of these intermediaries with respect to content created by their users. It is often argued that such frameworks that put these "intermediaries" or platforms at legal risk create a form of proxy censorship. The legal doctrine that governs such liability is based on the tort-law principle of secondary liability for third party action. These intermediaries who are third party defendants in various such actions understandably wonder why they should be made to pay for a third party's illegal acts and be forced to play complicit in a system that

[1] Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators (October – December 2013), available at* http://www.trai.go v.in/WriteReadData/PIRReport/Documents/Indicator%20Report s %20-%20Dec-2013.pdf (last visited April 1, 2014)

[2] The full report is available at http://www.iamai.in/rsh_pay.aspx?rid=rXiopaUzE7s= (last visited April 1, 2014); A news report is available at http://www.thehindu.com/news/national/80-million-social-media-users-by-nextelections/article4607051.ece (last visited July 13, 2014)

has the ability to suppress legal as well as illegal content, increasing their business costs to an unaffordable level.

In India, the Information Technology Act, 2000 lays down the legal framework for regulating the cyber-space. The Government of India notified the Information Technology (Intermediaries Guidelines) Rules, 2011 in April 2011 which laid down detailed procedures for regulation of intermediaries and online content. SFLC.IN had submitted feedback to the Government when the draft Rules were put up for consultation. However, when the final Rules were notified we found that most of our concerns were not addressed and that the Rules exceeded the scope of the parent act. A wide variety of people working in this area were of the view that some guidelines may be necessary to guide the users and the intermediaries about content take-down mechanisms, but the Rules in their current form could gravely harm the freedom of speech and expression and violate the right to privacy of citizens while undermining the constitutional right to practice a business or profession. These concerns were dismissed as mere theoretical speculations by the authors of the Rules. Therefore, to understand the issue in depth and provide real-life examples, we conducted detailed studies of the constitutionality of these Rules as well as a comparative study of the legislations in various countries. We also thought it was necessary to conduct widespread consultations to garner views on the issue from a cross-section of the society that included various interest groups. We hope that the findings of this study will assist the policy-makers in achieving the balance that they seek in preserving the rights guaranteed by the Constitution of India to its citizens while preserving the public order questions that they intend to address.

When the final Rules were notified we found that most of our concerns were not addressed and that the Rules exceeded the scope of the parent act.

1.1 Methodology

SFLC.IN organised four Round Table Consultations during May - June 2013 to address issues related to the Information Technology (Intermediaries Guidelines) Rules, 2011. We also invited people to submit their feedback on these Rules on our website. The consultations saw active participation from various stakeholders ranging from industry, civil society and academia. The purpose of organising these Round Table Consultations was to deliberate on the take-down mechanism established under the Intermediaries Guidelines Rules and the liability that intermediaries could face if they did not comply with these Rules. The major focus of the discussions was the chilling effect these Rules could have on the right to freedom of speech and expression on the Internet and on the ability to carry out business. To facilitate the process of consultation we also proposed draft Rules with a take-down and put-back mechanism.

Round Table Consultations were held at New Delhi, Mumbai, Bangalore and Cochin. These round table conferences were attended by representatives of intermediaries, industry associations, government, lawyers, civil society organisations and the general public. A list of all participants and their affiliations are uploaded on www.sflc.in along with this report.

The methodology followed by SFLC.IN in these Round Table consultations were:

a) Explanation of the concept of Intermediary Liability, its operation and the requirement of safe harbour provisions under the Information Technology Act, 2000.

b) Description of the procedure for take-down of third party content as laid down under the Information Technology (Intermediaries Guidelines) Rules, 2011.

c) Discussion on take-down scenarios mentioned by the participants.

d) Discussion on the guidelines proposed by SFLC.IN.

e) Recommendations by the attendees on the procedure for removal of content.

f) Eliciting responses to a Questionnaire on intermediary liability.

Based on the learnings of these consultations, we have made recommendations by incorporating the suggestions made by the attendees of these Round Table Consultations.

For easy reference, below is a summary of events that led to this report.

1.2 Time-line

Oct 17, 2000	Information Technology Act, 2000 came into force.
Oct 27, 2009	Information Technology (Amendment) Act, 2008 came into force. Section 79 of the Act provided safe harbour protection to intermediaries from liability arising out of user generated content.
Apr 11, 2011	Information Technology (Intermediaries Guidelines) Rules, 2011 notified.
Sep 6, 2011	Mr. Jayant Chaudhary, a Lok Sabha MP, spoke against the Rules in the Parliament and said that they curb the right to freedom of speech and are violative of the Information Technology Act, 2000.
Mar 1, 2012	Writ petition filed in the Kerala High Court challenging Rule 4 of Information Technology (Intermediaries Guidelines) Rules, 2011.
Mar 23, 2012	Motion to annul Information Technology (Intermediaries Guidelines) Rules, 2011 moved by Mr. P. Rajeeve in the Rajya Sabha.
May 9, 2012	Lucknow Bench of the Allahabad High Court directed the Government to implement the Information Technology (Intermediaries Guidelines) Rules, 2011 in their letter and spirit, in a writ petition in which the grievance was that many of the intermediaries were not disclosing the name of the grievance officers on their website.
May 17, 2012	Discussion on the Motion to annul the Rules took place in the Rajya Sabha. Mr. Arun Jaitley, the then Leader of oppostion, participating in the discussion stated that overly broad restrictions on the permissibility of on-line content would certainly constitute a threat to free speech. Mr. Kapil Sibal, Minister of Communications and Information Technology, replying to the annulment motion in the Rajya Sabha, assured the House that he will call for a discussion of all stakeholders. The motion was defeated.

"If the internet had been in existence, the internal emergency of 1975 would have been a big fiasco." - Mr. Arun Jaitley

Aug 2, 2012	Roundtable called by Mr. Kapil Sibal to discuss issues regarding Information Technology (Intermediaries Guidelines) Rules, 2011.
Nov 29, 2012	Meeting of the Cyber Rules Advisory Committee held.
Jan 25, 2013	Writ petition filed in the Supreme Court challenging Rules 3(2), 3(3), 3(4) and 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011 by Mr. Rajeev Chandrasekhar, a Member of Parliament in the Rajya Sabha. This is tagged with Shreya Singhal v Union of India (W.P(Crl) 167/2012), a Public Interest Litigation challenging Section 66 A of the Information Technology Act.
Mar 18, 2013	Department of Electronics and Information Technology (DEITY) issued a clarification on the Information Technology (Intermediaries Guidelines) Rules, 2011 stating that the intermediaries should respond within 36 hours and they should redress such complaints within one month.
Mar 21, 2013	Report of the Lok Sabha Committee on Subordinate Legislation suggested a fresh look at the Information Technology (Intermediaries Guidelines) Rules, 2011.
Apr 29, 2013	The Supreme Court admitted a writ petition filed by Mouthshut.com seeking to quash the Information Technology (Intermediaries Guidelines) Rules, 2011 and issued notices to the Central Government and a few State Governments. This was tagged with Shreya Singhal v Union of India and Rajeev Chandrasekhar v Union of India.
April 30, 2013	Round Table Consultation on Information Technology (Intermediaries Guidelines) Rules, 2011 held by SFLC.IN in New Delhi.
May 7, 2013	Round Table Consultation on Information Technology (Intermediaries Guidelines) Rules, 2011 held by SFLC.IN in Mumbai.
May 9, 2013	Round Table Consultation on Information Technology (Intermediaries Guidelines) Rules, 2011 held by SFLC.IN in Cochin.
May 10, 2013	Round Table Consultation on Information Technology (Intermediaries Guidelines) Rules, 2011 held by SFLC.IN in Bangalore.
Nov 22, 2013	The Supreme Court issued notice on a writ petition filed by People's Union for Civil Liberties (PUCL) challenging inter alia the Information Technology (Intermediaries Guidelines) Rules, 2011 and tagged it along with connected writ petitions.

2. Provisions of Information Technology Act, 2000 related to Intermediaries

The Information Technology Act, 2000 (IT Act) was introduced with the objective of providing legal recognition for transactions carried out by means of electronic commerce and to facilitate electronic filing of documents with the Government agencies. However, major changes were made to the Act by the Information Technology (Amendment) Act, 2008. This amendment clarified and expanded the definition of **intermediary** and gave them better protection from legal liabilities that could arise out of

user generated content. The expert committee[3] which gave inputs for the amendment has stated in its report that:

"Section 79 has been revised to bring-out explicitly the extent of liability of intermediary in certain cases. EU Directive on E-Commerce 2000/31/EC issued on June 8th 2000 has been used as guiding principles. Power to make rules w.r.t the functioning of the "Intermediary" including "Cyber Cafes" has been provided for under Section 87". However, this amendment was passed without much debate in the Lok Sabha on December 22, 2008 and in the Rajya Sabha on December 23, 2008.

2.1 Definition of Intermediary

Section 2(1)(w) of the Information Technology Act, 2000[4] **defines an intermediary** as **any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record**. Further, the definition of intermediary includes,

- telecom service providers,
- network service providers,
- internet service providers,
- web-hosting service providers,
- search engines,
- online payment sites,
- online-auction sites,
- online-market places, and
- cyber cafes.

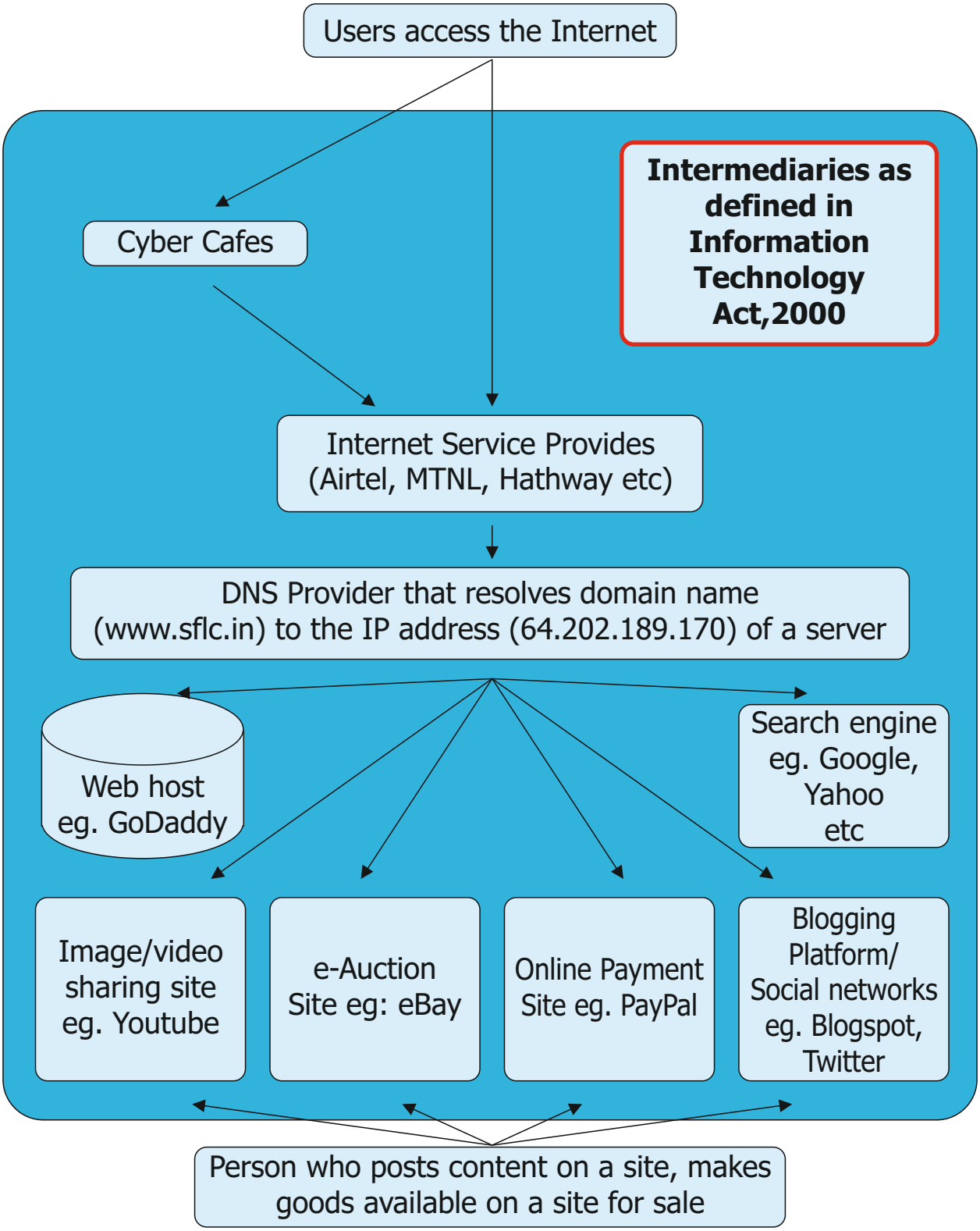
The amended definition of intermediary includes every person/entity who facilitates transactions between a recipient and a content provider.

[3] Department of Information Technology, *Report of the Expert Committee on Proposed Amendments to the Information Technology Act, 2000,* August 2005, *available at* http://www.deity.gov.in/sites/upload_files/dit/files/ downloads/itact2000/ITAct.doc (last visited on July 13, 2014)

[4] Section 2(1)(w), Information Technology Act, 2000:

"intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

Who is an Intermediary?



2.2 Safe Harbour under Section 79 of the Act

The intermediaries like ISPs, web hosts, social networking sites and blogging platforms play an important role in dissemination of information by providing tools and platforms that allow users to access the Internet, host content, share files and transact business. Websites like Blogspot, YouTube and Facebook provide a platform for users to post their content, but generally do not exercise editorial control over third-party user generated content.

Governments across the world realised that these intermediaries must be given protection from legal liability that could arise out of illegal content posted by users, considering the importance of these intermediaries in the online space and the fact that their mode of operation was quite different from the traditional brick-and-mortar business. Countries like the US, members of the European Union and India now provide protection to intermediaries from such user generated content. Such protection is often termed as a **'safe harbour' protection**.

The Act extends safe harbour protection only to those instances where the intermediary merely acts a facilitator and does not play any part in creation or modification of the data or information

Section 79 of the Information Technology Act, 2000[5] exempts intermediaries from liability in certain instances. It states that intermediaries will not be liable for any third party information, data or communication link made available by them. The Act extends safe harbour protection only to those instances where the intermediary merely acts a facilitator and does not play any part in creation or modification of the data or information. The provision also makes the safe-harbour protection contingent on the intermediary removing any unlawful content on its computer resource on being notified by the appropriate Government or its agency or upon receiving actual knowledge.

[5] Section 79, Information Technology Act, 2000:

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of subsection (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; *or*

(b) the intermediary does not

i. initiate the transmission,

ii. select the receiver of the transmission, and

iii. select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if—

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.—For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

This provision was added to the Act by the Information Technology (Amendment) Act, 2008 on the demand of the software industry and industry bodies to have protection from liability that could arise because of user generated content. This was mainly prompted by the controversial case[6] in which Avnish Bajaj, the CEO of Baazee.com, an auction portal, was arrested for an obscene MMS clip that was put up for sale on the site by a user.

The provision states that an intermediary needs to observe due diligence while discharging its duties under the Act and observe such other guidelines as prescribed by the Central Government. These other guidelines were laid down in the Information Technology (Intermediaries Guidelines) Rules, 2011 framed in the exercise of powers conferred by Section 87 read with subsection (2) of Section 79 of the Information Technology Act, 2000. The Rules were notified on April 11, 2011.

3. Analysis of the Intermediaries Guidelines Rules

The Intermediaries Guidelines Rules lay down the guidelines that the intermediaries have to follow so that they qualify for the safe-harbour protection provided under the Act.

3.1 Procedure for take-down of user generated content

The Intermediaries Guidelines Rules lay down the procedures that an intermediary has to follow to avail safe harbour. Rule 3(2)[7] of the Intermediaries Guidelines Rules lists the categories of information, if posted online, which could be considered as illegal. According to Rule 3(4)[8] an affected person could write to the intermediary to remove any content which is listed as unlawful under Rule 3(2). The intermediary has to act within 36 hours to remove the content. If the intermediary does not act within the stipulated time then the intermediary cannot avail safe harbour.

If the intermediary does not act within the stipulated time then the intermediary cannot avail safe harbour.

[6] *Avnish Bajaj v. State*, 150 (2008) DLT 769 and *Aneeta Hada v. Godfather Travels and Tours Pvt. Ltd.*, AIR 2012 SC 2795

[7] Rule 3(2), Information Technology (Intermediaries Guidelines) Rules, 2011:

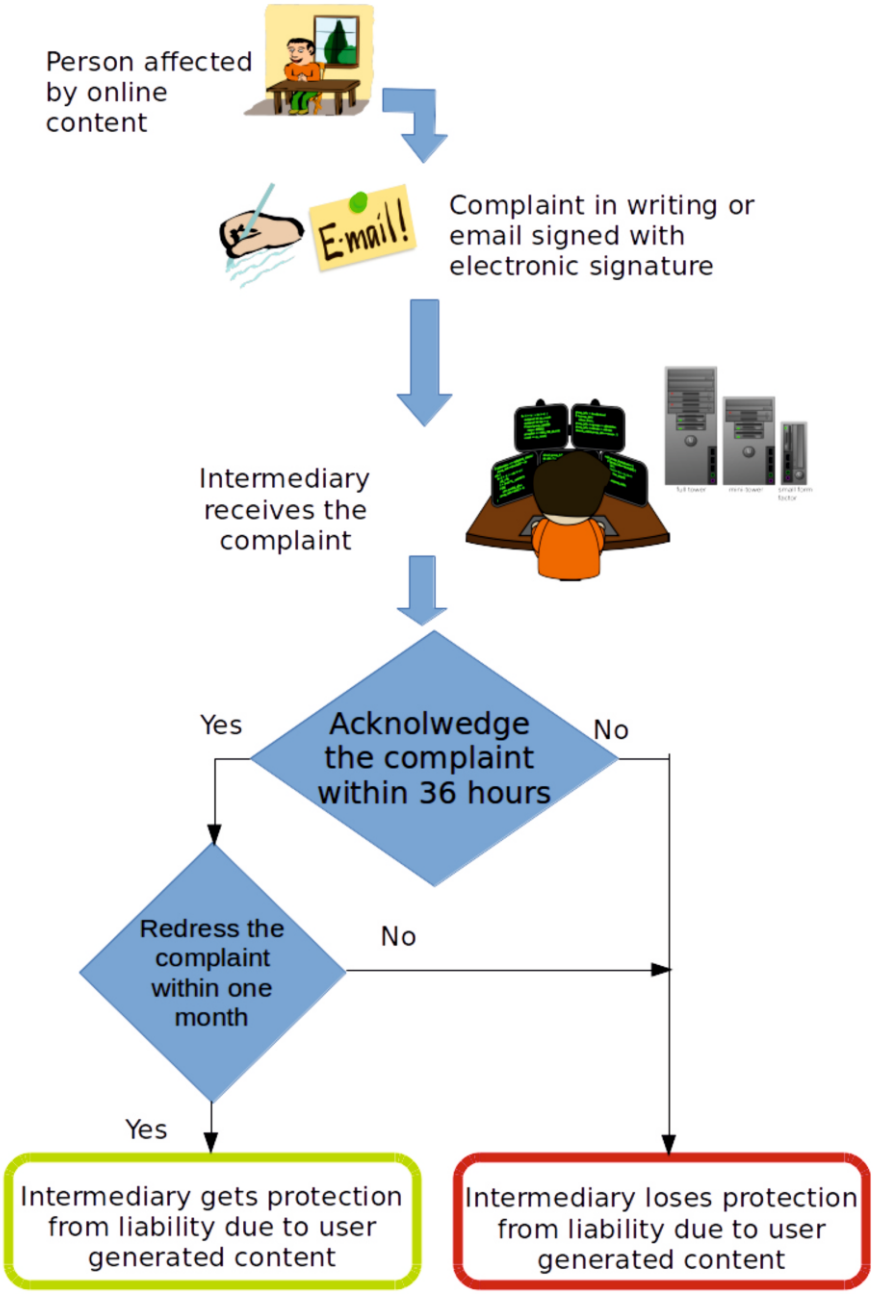
Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —
(a) belongs to another person and to which the user does not have any right to;
(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
(c) harm minors in any way;
(d) infringes any patent, trademark, copyright or other proprietary rights;
(e) violates any law for the time being in force;
(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
(g) impersonate another person;

[8] Rule 3(4), Information Technology (Intermediaries Guidelines) Rules, 2011:

The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.

This provision was criticised by intermediaries who said that it is not easy to take down content or take action in 36 (thirty six) hours. Thereafter, a clarification[9] was issued by the Government on March 18, 2013 stating that the intermediary shall respond or acknowledge the complaint within 36 hours. Thereafter, the intermediary has 30 (thirty) days time to redress such complaints. What constitutes redressal is unclear and no guidance has been provided by the rules.

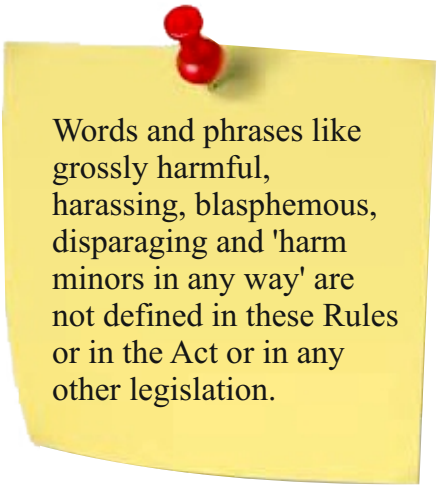
The Information Technology (Intermediary Guidelines) Rules, 2011 make it obligatory for intermediaries to appoint a grievance officer and provide the name and contact details of such officer on their website. The grievance officer shall redress the complaints within 30 days from the receipt of complaint.



[9] Department of Electronics & Information Technology, *Clarification on the Information Technology (Intermediaries Guidelines) Rules, 2011 under Section 79 of the Information Technology Act, 2000* (March 18, 2013), available at http://deity.gov.in/sites/upload_files/dit/files/Clarification%2079rules%281%29.pdf, (last visited April 1, 2014)

3.2 The Rules - Opinions of users and businesses

The users as well as the industry have criticised the Rules for the provisions that affect freedom of expression of citizens as well as the ability of businesses to operate and provide online platforms for sharing content. The following issues have emerged from the consultations held by SFLC.IN.



3.2.1 Uncertainty regarding prohibited content

The ambiguous words used in Rule 3(2) on the nature of content that should not be posted by users make it difficult for the users as well as for the intermediaries to determine the type of content that will be classified as objectionable. **Words and phrases like grossly harmful, harassing, blasphemous, disparaging and 'harm minors in any way' are not defined** in these Rules or in the Act or in any other legislation. These ambiguous words make the Rules susceptible to misuse. Such ambiguous terms have a *chilling effect* on free speech rights of users by making them too cautious about the content they post and by forcing them to self-censor. This will have an adverse impact, especially on political discourse and views critical of acceptable main-stream ideas. A major casualty of such Rules could be discussions on sexuality, gender rights, rights of lesbians, gays and trans-genders, criticisms of religious practices and honest political discourse. The absence of such discussions is detrimental to the healthy functioning of an open and honest society and will sound the death knell of democracy. This is evident from the reported instances in the short period in which the Rules have been in operation.

Mouthshut.com, India's leading consumer review website revealed to SFLC.IN that they receive a large number of take-down requests from businesses to take down unfavourable reviews posted by customers. Faisal Farooqui, CEO, MouthShut.com said that they have received a number of notices from law enforcement agencies under Section 91 of Cr.PC and that there were instances where they were sent fake court orders demanding take down of content. The Centre For Internet and Society, a non-profit organisation based out of Bangalore, as part of the research study, sent a number of take-down requests targeting perfectly legal content and six out of seven intermediaries over-complied with the notices. In another instance, the website cartoonsagainstcorruption.com was taken down by the domain registrar, Big Rock (*Big Rock has explained their stance on the issue in the blog post available at http://bigrock.com/blog/general/cartoons against corruption-combigrocksstance-and-a- sequence-of-events*) on receiving a legal notice from the Cyber Police Station, Crime Branch, CID, Mumbai by relying on the provisions of these Rules. In yet another instance, Vidyut Kale, a blogger, was served a legal notice under the Rules asking her to take down a post[10] that she had written about a corruption scandal. Although a blogger will not come under the definition of an intermediary in this instance, this incident clearly shows how the Rules are susceptible to be used to restrict the freedom of users to voice opinions.

[10] *The post published at https://aamjanata.com/sailgate-the-party-that-wasnt/, was taken down on receiving a takedown notice. The blogger has uploaded a copy of the take-down notice here(last visited July 13, 2014)*

Although we tried to get information on content taken down by major intermediaries like Facebook and Google, we were not provided this information and were requested to get information from their transparency reports. However these reports do not provide much information about take downs due to requests from private individuals and mainly provide consolidated numbers of take-down requests from Government agencies.

Intermediaries, who have to make decisions as to whether any complaint about content posted falls under these categories of content, are often constrained by the use of ambiguous terms and are forced to take the safe course of taking down all content - the removal of which has been requested.

3.2.2 Rights of content-creators

The take-down mechanism under the Rules **does not provide any recourse to the creator of content whose content has been taken down on the basis of a complaint.** There are no provisions that make it mandatory to inform the content creator of the removal of content posted by her.

The take-down mechanism under the Rules does not provide any recourse to the creator of content whose content has been taken down on the basis of a complaint.

No Information Mechanism: The content-creator need not even be informed about the complaint by the intermediary and she does not get a chance to state her case and to object to the take-down. Sometimes, for days, the content-creator has no inkling that her content has been removed.

No Redressal Mechanism: The Rules do not have any redressal mechanism for the content creator who is aggrieved by a wrongful take-down of content. The Rules do not have a putback mechanism to restore the content that may have been wrongfully or mistakenly taken down. Considering the importance of the Internet and the platform it provides for citizens to voice their opinions and participate in the current discourse, the freedom of expression of users will be severely hampered if their content is taken down by the intermediary on receipt of a take-down notice without any recourse.

The intermediaries are obliged to take a final decision on the lawful nature of the content posted.

3.2.3 Adjudicatory role to intermediaries

The intermediaries are obliged to take a final decision on the lawful nature of the content posted. The Rules do not have a provision mandating the complainant to get a court order. The Rules in the current form do not have a provision for judicial scrutiny. This is in stark contrast with the provision in the amended Copyright Act, which necessitates production of a court order within a period of twenty one days on take-down of an allegedly infringing content. No justification is forthcoming on this discrepancy.

The take-down of content should, at best, be an interim measure to protect the interest of the aggrieved party with the courts having a final say.

3.2.4 Operational difficulty for Industry

The Rules by mandating an adjudicatory role for the intermediaries have made it difficult for various websites for example, customer review sites to operate. In a country where consumer protection laws are difficult to enforce, where the common man is duped everyday, websites enabling views and reviews about goods and services provide an important public service.

Business model of these websites centres around the freedom of users to express honest views of products and services and frequent take-down of content and sanitized reviews will make customers reluctant to use these services, thereby affecting their business. The ambiguous words used in the Rules compound the problems of these sites by making them err on the side of caution and to even take down content that is not unlawful. The consultations held by SFLC.IN revealed that ***many of the businesses were not aware of the clarification issued by the Government on the time period*** within which they have to take action and they considered it mandatory to take down the content within a period of thirtysix hours on receipt of notice. The Hon'ble Delhi High Court while passing an interim order dated March 30, 2012 in *Nirmaljit Singh Narula v. Indijobs at hubpages.com & Ors.*[11] held that "*Rule 3(4) of the said rule provides obligation of an intermediary to remove such defamatory content within 36 hours from receipt of actual knowledge.*" The Hon'ble Court went on to restrain the intermediary, hubpages.com, from hosting any defamatory content about the plaintiff and if the order is not complied within 36 hours to get the website blocked. Although this order was passed before the clarification was issued by the Government, it clearly shows how the Rules are often interpreted. At the consultation held in Mumbai, MouthShut.com informed the attendees that they were getting an unusually large number of notices from builders, banks and other commercial establishments who want negative reviews about their organisation to be taken down and that such notices are often followed by court cases if they do not take down the content. MouthShut.com stated that they are forced to defend cases across the country and that their legal expenses have gone up. They said that they have received 790 take down requests, 240 legal notices and were fighting 11 court cases, as on that date.

Business model of these websites centres around the freedom of users to express honest views of products and services and frequent takedown of content and sanitized reviews will make customers reluctant to use these services, thereby affecting their business.

3.2.5 Privacy of users

In the wake of the recent disclosures about arbitrary surveillance of users, Rule 3(7) of these Rules that mandate the intermediaries to disclose private information of users on getting a written request alone from any investigative agency is problematic as the law enforcement agency can access user records without complying with any safeguards to protect user privacy as provided in the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. Such over-broad provisions without adequate safeguards could result in violation of the right to privacy of users.

[11] 190 (2012) DLT 51

The Controller of Certifying Authorities had resorted to Rule 3(7) of the Rules to demand Yahoo India Pvt. Ltd. to hand over user data. Yahoo India Pvt. Ltd. challenged the action of the Controller imposing a fine for not revealing user data as well as Rule 3(7) of these Rules before the Hon'ble High Court of Delhi.[12] The Hon'ble High Court allowed the writ petition by setting aside the order of the Controller and leaving the question open on the challenge to Rule 3(7). Mouthshut.com revealed during the Round Table Consultation held by SFLC.IN that they have received requests from law enforcement agencies to reveal user information, often citing alleged non-cognizable offences like defamation.

Such over-broad provisions without adequate safeguards could result in violation of the right to privacy of users.

3.3 Differentiating private take-down from the government's powers for blocking access

In debates on intermediary liability, a concern often raised is the need for a mechanism to take down content quickly in the case of content that could affect communal harmony or national security. An instance often cited is the Bangalore exodus of persons from the North-eastern region of the country allegedly spurred by offensive text messages and posts on social media.[13] However, this argument overlooks the fact that there is a separate provision under Section 69A of the Information Technology Act, 2000 and the Rules notified under it to deal with it. This provision empowers the Government to act in cases where the content is of a nature that could affect the sovereignty and integrity of the nation or affect public order. The provision is quoted below:

Section 69A: Power to issue directions for blocking public access of any information through any computer resource.—*(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing by order, direct any agency of the Government or intermediary to block for access by the public any information generated, transmitted, received or stored in any computer resource.*

The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 mandate the procedures for such blocking. Rule 9 of these Rules enables the Designated Officer to take immediate steps in cases of emergency. Thus, the Government has ample power at its disposal to deal with illegal content that could lead to law and order problems.

3.4 Need for a private take-down mechanism

During the consultations held by SFLC.IN, the following reasons were cited by some participants to have a take-down mechanism under the control of the intermediaries:

1. Due to the vast amount of information updated on sites hosting user generated content like the social media sites, Government will not be in a position to take action on complaints

[12] *Yahoo India Pvt. Ltd. V Union of India & Another*, W.P.(C).No. 6654/2011

[13] Sharath S Srivasta & Deepa Kurup, *After rumours northeast People flee Bangalore*, THE HINDU, (Aug. 16, 2012), *available at* http://www.thehindu.com/news/national/karnataka/after-rumours-northeast-people-fleebangalore/ article3776549.ece (last visited July 13, 2014)

received from aggrieved persons under Section 69A of the IT Act.

2. There are instances where privacy of individuals are breached due to uploading of their obscene photographs by others which demands quick action.

However, the participants also expressed the view that this kind of take-down should be limited to extreme cases and proper safeguards need to be incorporated to prevent this mechanism degenerating into a private censorship mechanism. The safeguards should ensure that the restrictions on content are limited to the reasonable restrictions listed under Article 19(2) of the Constitution and that the rights of the content-creators are also protected.

3.5 Legal analysis of the Rules

The Information Technology (Intermediaries Guidelines) Rules, 2011 prescribing guidelines to be observed by the intermediaries were issued by the Central Government in exercise of the powers conferred by clause (zg) of subsection (2) of Section 87 read with sub-section (2) of Section 79 of the Information Technology Act, 2000 (Act 21 of 2000) .

Section 79 of the Act as amended in 2008 provides intermediaries protection from liability arising out of user generated content. This is in line with the position followed in countries like the US and members of the European Union ("EU"). The Digital Millennium Copyright Act[14] and the Communications Decency Act[15] in the US and the Directive on Electronic Commerce in the EU provides protection to intermediaries from liability arising out of content posted by users of services provided by intermediaries.

The provisions of the Rules that could be unconstitutional or ultra vires of the parent act are listed below:

3.5.1 Sub-rule (2) of Rule 3

Ambiguous Terms

Rule 3(2) mandates intermediaries to place restrictions on the kind of content that a user can post by mandating it in the rules and regulations, terms and conditions or user agreement. Rule 3(2) mandates terms and agreements to inform users not to host information included in a broad list that includes information that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever.

The Rule could be held to be arbitrary and violative of Article 14 of the Constitution of India.

The subject matter of information listed in this rule including words like:

- blasphemous,
- grossly harmful,
- harassing,

[14] Digital Millennium Copyright Act, *available at* http://www.copyright.gov/title17/92chap5.html#512 (last visited April 1, 2014)

[15] Copyright Act, *available at* http://www.law.cornell.edu/uscode/text/47/230, (last visited April1, 2014)

- invasive of another's privacy,
- racially, ethnically objectionable,
- disparaging,
- belongs to another person and
- harm minors in any way,

is highly subjective and is not defined either in the Rules or in the Act, or in any statute for that matter. The Rule by including such ambiguous terms results in wide interpretation of the subject matter, and hence, the Rule could be held to be arbitrary and violative of Article 14 of the Constitution of India.

Violative of Article 19(2)

Clause (2) of Article 19 of the Constitution of India permits the State to make laws mandating reasonable restrictions on the exercise of the right conferred by Article 19(1)(a) in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence. Thus, any restrictions that can be imposed on the right of citizens to freedom of speech and expression can only be within the ambit of clause (2) of Article 19.

Clause (I) of Rule 3(2) has listed the reasonable restrictions to freedom of speech permissible under Article 19(2) of the Constitution of India. Apart from clause (i) of Rule 3(2), **all the clauses attempt to impose restrictions that are beyond what can be imposed under Article 19(2).** The Hon'ble Supreme Court has held in *Express Newspapers (Private) Ltd. and Anr. Vs. The Union of India (UOI) and Ors.*[16], that if any limitation on the exercise of the fundamental right under Art. 19(1)(a) does not fall within the four corners of Article 19(2) it cannot be upheld. Thus, these restrictions that are imposed are violative of the constitutional provisions.

3.5.2 Sub-rule (4) of Rule 3

Violative of Principles of Natural Justice

Rule 3(4) that mandates that the intermediary, upon obtaining knowledge by itself or being brought to actual knowledge by an affected person about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours to disable such information that is in contravention of sub-rule (2), does not provide for an opportunity to the user who has posted the content to reply to the complaint and to justify his case. The Government subsequently clarified the procedure that needs to be implemented. The clarification stated that the intermediary shall respond to or acknowledge the complaint within 36 hours. Thereafter the intermediary has 30 days to redress such complaints. The Rule, which mandates the intermediary to disable the content without providing an opportunity of hearing to the user who posted the content, is violative

> The Rules place a burden on the intermediaries to decide on the lawful nature of the content as a pre-condition for exemption from liability.

[16] AIR 1958 SC 578

of the principles of natural justice and is highly arbitrary. This provision results in taking down of content without any involvement of the executive or the judiciary without any checks and safeguards. **This Rule results in endowing an adjudicatory role to the intermediary in deciding questions of fact and law, which can only be done by a competent court. Such a provision of the Rules is liable to be misused and is thus arbitrary.**

The Rules place a burden on the intermediaries to decide on the lawful nature of the content as a pre-condition for exemption from liability. The intermediaries, on receiving a complaint, in order to ensure that they continue to receive the protection offered by Section 79 of the Act, will be forced to acknowledge the complaint within 36 hours and to redress the grievance within one month. The intermediary will often be forced to take the easier route of take-down of content than get embroiled in a legal action on standing by the content-creator. Thus, the direct effect of the Rules will be strict censoring of content posted on-line by users. The Rules will have a direct effect on the fundamental right of freedom of speech and expression guaranteed under Article 19(1) of the Constitution of India.

Censorship by Proxy

Clause (b) of sub-section 3 of Section 79 of the Information Technology Act, 2000 mandates the intermediary, on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, to disable access to the material. The Rule has in effect amended this provision by providing for any affected person to submit a request to the intermediary to take down content and mandating the intermediary to act on the request within a period of 36 hours. This provision, which results in taking down of content without any involvement of the Government or its agency, leads to a private censorship mechanism without any checks and safeguards.

Section 69A of the Information Technology Act, 2000 provides that when the Central Government or any of its officers specially authorised by it in this behalf, is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may, subject to the provisions of sub-section (2) of Section 69A, and for reasons to be recorded in writing by order, direct any agency of the Government or intermediary to block for access by the public any information generated, transmitted, received or stored in any computer resource. The legislature has thus spelt out a specific procedure for blocking access to information. The Central Government has notified the Rules providing for safeguards for such blocking of access called the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. The Rules lay down the procedure and safeguards for blocking of access of any information that comes under the scope of sub-section (1) of Section 69A. Rule 3(4) of the intermediary Rules is in

> Rule 3(4) of the intermediary Rules is in direct contravention of Section 69 A of the Act

direct contravention of Section 69 A of the Act and the Rules made thereunder and is hence ultra vires of the Act.

3.5.3 Sub-rule (5) of Rule 3

Rule 3(5) mandates the intermediary to inform users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the intermediary has the right to immediately terminate access or usage rights of users to the computer resource of the intermediary and remove non-compliant information. This provision will result in termination of services to a user on posting of any content which the intermediary deems as unlawful without actually notifying the user of the reason for such termination. This provision does not provide for any checks and balances for use of this power to terminate the access of a user. Such a power mandated to be exercised by the intermediary is arbitrary.

The right to freedom of speech and expression guaranteed by the Constitution includes the right to receive information. Article 19(2) of the International Covenant on Civil and Political Rights states that "*Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.* " The Hon'ble Supreme Court has held in *People's Union of Civil Liberties (PUCL) v. Union of India (UOI) and Anr.*[17], that *"It is almost an accepted proposition of law that the rules of customary international law which are not contrary to the municipal law shall be deemed to be incorporated in the domestic law".*

The disconnection of the service by an intermediary will affect the right of a citizen to receive information and this is a violation of the fundamental right under Article 19(1) of the Constitution of India. The Hon'ble Supreme Court has held in *The Secretary, Ministry of Information & Broadcasting v Cricket Association Of Bengal*[18], that:

"*The freedom of speech and expression includes right to acquire information and to disseminate it. Freedom of speech and expression is necessary, for self expression which is an important means of free conscience and self fulfillment. It enables people to contribute to debates of social and moral issues. It is the best way to find a truest model of anything, since it is only through it, that the widest possible range of ideas can circulate. It is the only vehicle of political discourse so essential to democracy. Equally important is the role it plays in facilitating artistic and scholarly endeavours of all sorts. The right to communicate, therefore, includes right to communicate through any media that is available whether print or electronic or audio-visual such as advertisement, movie, article, speech etc. That is why freedom of speech and expression includes freedom of the press. The freedom of the press in terms includes right to circulate and also to determine the volume of such circulation. This freedom includes the freedom to communicate or circulate one's opinion without interference to as large a population in the country as well as a broad as impossible to reach.*"

In *Tata Press Ltd. Vs. Mahanagar Telephone Nigam Limited and Ors*[19], the Hon'ble Supreme Court held that:

[17] (1997)1 SCC 301
[18] 1995 AIR SC 1236
[19] (1995) 5 SCC 139

sflc.in

"*Article 19(1)(a)not only guarantees freedom of speech and expression, it also protects the rights of an individual to listen, read and receive the said speech.*"

Rule 3(5) by providing for terminating access to the services of an intermediary without laying down any procedures and safeguards, results in violation of a citizen's right to freedom of speech and expression.

3.5.4 Sub-rule (7) of Rule 3

Rule 3(7) mandates the intermediary, when required by lawful order, to provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The requirement for lawful order is modified while mandating that the information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance. The requirement of giving information about users by the intermediary on a mere written request from an agency could have serious implications on the right to privacy of citizens. Right to privacy as a component of Article 21 of the Constitution of India, which guarantees for "right to life and personal liberty" has been recognised by the Hon'ble Supreme Court in *Gobind v. State of Madhya Pradesh*[20], and *R. Raj Gopal v. State of Tamil Nadu*[21]. This right can be curtailed only by a procedure established by law and cannot be done arbitrarily. The Hon'ble Supreme Court of India in *People's Union of Civil Liberties (PUCL) v. Union of India (UOI) and Anr.*[22], while deliberating on the issue of tapping of telephone conversation held that "Telephone-Tapping is a serious invasion of an individual's privacy" and prescribed guidelines for that. In the case of communications using Internet, communications like email and chat messages are often stored on servers by the service providers and on accessing the user accounts on these servers, a user's entire communication can be accessed. Thus, the Rules by providing for information to be provided by intermediaries on a written request results in wire-tapping of the Internet without any legal safeguards whatsoever.

The requirement of giving information about users by the intermediary on a mere written request from an agency could have serious implications on the right to privacy of citizens.

Section 69 of the Information Technology Act, 2000 deals with the power to issue directions for interception or monitoring or decryption of any information through any computer resource. Sub-section (2) of Section 69 provides for procedures and safeguards subject to which such interception or monitoring may be carried out. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were notified by the Government to provide for such safeguards and procedures. These Rules enshrine the guidelines prescribed by the Hon'ble Supreme Court in *People's Union of Civil*

[20] (1975) 2 SCC 148

[21] (1994) 6 SCC 632

[22] (1997)1 SCC 301

Liberties (PUCL) Vs. Union of India (UOI) and Anr.[23] These Rules mandate that such interception or monitoring of information can be carried out only by an order issued by a competent authority. The competent authority to issue such an order under these Rules is the Secretary in the Ministry of Home Affairs, in case of Central Government or the Secretary in charge of the Home Department, in case of a State Government or Union Territory. Rule3(7) that mandates an intermediary to provide information does not have any such safeguards and is in violation of the provisions of the Act and the Rules issued thereunder.

3.6 Safe-harbour and Take-down mechanism in the Copyright Act

The Copyright (Amendment) Act, 2012 added a provision providing safe-harbour protection to those providing transient or incidental storage of a work or performance. Section 52(c) of the amended Act provides that if the person responsible for the storage of the copy has received a written complaint from the owner of copyright in the work, complaining of infringement, he shall refrain from facilitating such access for a period of twenty-one days or till he receives an order from the competent court refraining from facilitating access. It further provides that in case no such order is received before the expiry of such period of twenty-one days, he may continue to provide the facility of such access. Thus, the take-down mechanism envisaged in the Copyright Act makes it obligatory for the complainant to produce an order from a competent court within a period of twenty one days, failing which the content may be put back by the service provider. However, the Intermediaries Guidelines Rules do not have such a stipulation for production of a Court order.

The take-down mechanism envisaged in the Copyright Act makes it obligatory for the complainant to produce an order from a competent court within a period of twenty one days, failing which the content may be put back by the service provider.

Rule 75(4) of the Copyright Rules, 2013 also mandates displaying of a notice giving reasons for restraining access to persons requesting access to the alleged infringing copy. Such a stipulation regarding display of notice of the content taken down based on a complaint is not provided for in the Intermediaries Guidelines Rules. There is no justification forthcoming as to why removal of content on the grounds of copyright violation requires a court order but the removal on any other "objectionable " grounds does not.

3.7 Comparison of legislations in other countries on Intermediary Liability

3.7.1 United Kingdom

In the United Kingdom, intermediaries are classified based on the provisions in the Electronic Commerce (EC Directive) Regulations, 2002[24] which transposed the provisions in Directive 2000/31/EC[25] of the European Parliament, commonly known as the E-commerce Directive.

Under the E-commerce Directive, a website provider has a defence against liability for illegal acts carried out by third party services, if it is acting as a mere conduit, cache or host of information, and:

[23] Supra. 20

[24] Electronic Commerce Regulations, 2002, *available at* http://www.legislation.gov.uk/cy/uksi/2002/2013/made, (last visited July 13, 2014)

[25] Directive 2000/31/EC of the European Parliament, *available at* http://eurlex.europa.eu/legalcontent/EN/ALL/;ELX_SESSIONID=52sgTQFGkhW0f3cPl3MSrDfmWKb1gzbg4DY7pyMvQvbYySHFSmqz!-735511499?uri=CELEX:32000L0031, (last visited July 13, 2014)

1. as a **mere conduit**, it does not initiate or modify the transmission, or store information other than as necessary for transmission;

2. as a **host**, it has no actual knowledge of any illegal activity, and on obtaining such knowledge, acts expeditiously to remove or disable access to the information; and

3. as a **cache**, it does not modify the information, and, on obtaining knowledge of the illegal activity, acts expeditiously to remove or disable access to the information.

The Regulations lay out standards to determine 'actual knowledge' of the intermediary by stating that in determining whether there was actual knowledge (of an infringing action), a court is to take into account all matters which appear to it in the particular circumstances to be relevant, including,

a) whether a service provider has received a notice through a means of contact made available by the intermediary, and

b) the extent to which any notice includes the full name and address of the sender of the notice, details of the location of the information in question, and details of the unlawful nature of the activity or information in question.

There is no formal notice and take-down mechanism in UK. Apart from the Defamation Act, 2013[26] and practices recommended by organizations that issue self regulatory code of practices. The Defamation (Operators of Websites) Regulations 2013[27]under the Defamation Act have created a notice and take-down mechanism for defamatory content. Section 5 of the Act introduces a new defence for the operators of websites who can show that they were not responsible for the posting of material on their site. This will primarily apply to the operators of forums and blog sites but will be relevant for all sites, which encourage user-generated content. The defence will be defeated if the claimant can show that (1) it was not possible to identify the actual poster; (2) they gave the operator a notice of complaint; and (3) the operator failed to respond in accordance with a procedure to be set out in forthcoming regulations. The claimant is deemed to have sufficient information to "identify" the poster if he has sufficient information to bring proceedings against him.

The Regulations under the Defamation Act set out actions website operators must take when notified of the existence of defamatory comments on their site in order to avoid becoming liable for that material:

1. Website operators seeking to avoid liability for defamatory comments published on their sites would have two days, in general, to notify the authors of those comments about complaints they receive under new legislation drafted by the Government.

2. Upon notification, authors of the comments would have five days to issue a written response outlining whether they consent to the removal of the comments from the site. A failure to respond would place website operators under the obligation to delete the comments within 48 hours of that five day deadline expiring if they are to avoid exposure to liability.

[26] Defamation Act, 2013, *available at* http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted, (last visited July 13, 2014)

[27] Defamation (Operators of Websites) Regulations, 2013, *available at* http://www.legislation.gov.uk/ukdsi/2013/9780111104620, (last visited April 1, 2014)

3. When notifying authors that their comments are subject to defamation complaints, website operators would have to conceal the identity of the complainant from those authors if such anonymisation is sought by the complainants.

4. In cases where the authors do not consent to the removal of their comments, those individuals or businesses would be required to inform website operators of their name and address and tell the operator whether or not they consent to the handing over their details to the complainant. A complainant would have to be informed by the operator within 48 hours of an author's response and of the content of that response.

5. Website operators would be required to delete comments from their site within two days of receiving a notice of complaint if it has "no means of contacting the poster" through a "private electronic communication" channel, such as via email.

6. If authors that do respond to website operators' notifications of a complaint fail to provide details of their full name and address, the operators would have to remove their comments within two days of that response. If a "reasonable website operator" believes that details given by an author are "obviously false" then they must also delete the comments within the 48 hour deadline.

7. In cases where authors of defamatory comments repost the same or substantially similar comments after they have been removed twice before from the site, website operators would be obliged to remove the comments within 48 hours of receiving a notice of complaint.

United Kingdom also has many self-regulatory codes of practice. The Internet Watch Foundation(IWF) is a self-regulatory body that was established in 1996 by the Internet industry to provide the United Kingdom Internet Hotline for the public and IT professionals to report criminal online content in a secure and confidential way. It works in partnership with the online industry, the Government, and international partners to minimize the availability of obscene content, specifically:

1. Child abuse images hosted anywhere in the world
2. Criminally obscene adult content hosted in the UK
3. Non-photographic child sexual abuse images hosted in the UK.

The Code of Practice of the IWF defines a 'Notice and Takedown' procedure by which service providers remove or disable access to potentially illegal content hosted on their networks or on Usenet Services they provide, following receipts of a Notice from the IWF.

3.7.2 The United States of America

In the United States, the online intermediaries get protection from liability arising out of user generated content as the law does not treat them as publishers. Section 230 of the Communications Decency Act[28] gives immunity to intermediaries by not treating them as publishers. The relevant clause of the section states

The Communications Decency Act gives immunity to intermediaries by not treating them as publishers.

[28] Section 230, Communications Decency Act, available at http://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/html/USCODE-2011-title47-chap5-subchapII-partI-sec230.htm (last visited July 13, 2014)

that 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.

In the case of take- down of content based on alleged infringement of copyright, the relevant legislation in the U.S. is the Digital Millennium Copyright Act[29], commonly referred to as DMCA. Online Copyright Infringement Liability Limitation Act, Title II of DMCA, has a notice and counter-notice mechanism. The Act provides a safe-harbour for online service providers(OSP), provided they comply with the terms of the legislation. As per the notice provision, the copyright holder or his agent, on noticing an infringing material online can send a notice with details of the work, the address of the infringing material, contact information and a statement under penalty of perjury to the designated agent of the online service provider. The OSP has to disable access to the infringing material and inform the person who posted the infringing material about the receipt of the take-down notice. The person who posted the material can then file a counter-notice. The OSP on receipt of the counter-notice has to inform the complainant. If the complainant does not respond by informing the OSP of his filing a lawsuit, the OSP has to restore the content within a minimum period of 10 days and a maximum period of 14 days.

DMCA safe harbours extends safe harbour protection only to four types of intermediaries:

1. conduit providers such as telephone companies,
2. those who store or cache content hosted by another,
3. those who host content posted by another,
4. search engines.

Safe harbour is only extended to an intermediary that "does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.

Trademark Act, 1946 (Title 15, United States Code, Section 1114) under Section 32[30] provides a safe harbour from trademark infringement for publishers, which is also extended to online providers of content written by another.

3.7.3 Australia

Copyright

The Copyright Regulations 1969[31] mandates the procedure for take-down of content which infringes copyright. The procedure is spelt out in Regulations 20J, 20K, 20L and 20M. Upon receiving the notice of infringing content, the carriage service provider has to remove or disable access to infringing content. The service provider has to inform the user who uploaded the content about the take-down and provide him a copy of the notice of claimed infringement. The user may issue a counter-notice within 3 months of receipt of this notice. The copyright owner or agent has to notify the designated agent of the provider within 10 days that action seeking a court order has been taken to restrain the infringement. If such information is not received the content must be restored by the service provider.

The Copyright Act 1968 provides safe harbour protection only to 'internet service providers'

[29] Supra. 13

[30] Section 32, Trademark Act, 1946, *available at* http://www.uspto.gov/trademarks/law/Trademark_Statutes.pdf (last visited July 13, 2014)

[31] Copyright Regulations, 1969, *available at* http://www.austlii.edu.au/au/legis/cth/consol_reg/cr1969242/s20j.html, (last visited July 13, 2014)

The Copyright Act 1968[32] provides safe harbour protection only to 'internet service providers'[33]. A classification of intermediaries in Section 116AC – 116AF is as follows:

– providing facilities or services of transmitting, routing or providing connection for copyright material, or immediate and transient storage of copyright material in the course of transmission, routing or provision of connections.*(mere conduit)*

– caching copyright material through an automatic process, the material for caching must not be automatically selected by the intermediary.

– storing, at the direction of a user, copyright material on a system or network controlled or operated by or for the intermediary.

– Referring to users an online location using information location tools or technology

The liability of the above intermediaries is limited to injunctive relief. Further, the kind of remedies available also depends on the kind of services provided by an intermediary. For eg. A *mere conduit* shall be required to take reasonable steps in disabling access to infringing copyright material to an online location outside Australia, whereas all the other catergories of intermediaries shall be required to remove or disable access to infringing copyright material or to a reference to infringing copyright material (Section 116AG)

In order to avail the safe harbour protection, intermediaries must satisfy the conditions as put forth under Section 116AH(1) i.e. to have a policy under which the accounts of repeat infringers shall be terminated. Where an intermediary carries out the function of 'hosting' or providing ' location tools', and if the intermediary has the right and ability to control the activity, no financial benefit that is directly attributable to the infringing material shall be received by the intermediaries, this is another condition imposed by the Section 116AH in order to avail safe harbour protection.

Prohibited content

Australia follows a co-regulatory model for regulating content on the Interent. The Broadcasting Services Amendment (Online Services) Act 1999[34] (which amends the Broadcasting Services Act 1992) has established the authority of the Australian Communications and Media Authority (ACMA) to regulate Internet content and issue take down notices on receiving complaints from individuals. The ACMA is not mandated to scour the Internet for potentially prohibited content, but it is allowed to begin investigations without an outside complaint.

ACMA directs service providers to take-down content based on the classification scheme for the content[35]. This classification[36] is the same as that for broadcast, print and visual media. The content which is prohibited under this classification is limited to content involving sex, drug misuse and violence. e.g, Films that depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality , decency and propriety generally accepted by reasonable adults to the extent

[32] Copyright Act, 1968, *available at* http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/ (last visited July 13, 2014)

[33] *Inserted by* US Free Trade Agreement Implementation Act 2004 – Schedule 9, *available at* http://www.austlii.edu.au/au/legis/cth/consol_act/uftaia2004363/sch9.html (last visited July 13, 2014), *amended by* the Copyright Legislation Amendment Act, 2004 No. 154, 2004- Schedule 1, *available at* http://www.austlii.edu.au/au/legis/cth/num_act/claa2004325/sch1.html (last visited July 13, 2014)

[34] Broadcasting Services Amendment (Online Services) Act, 1999, *available at* http://www.comlaw.gov.au/Details/C2004A00484 (last visited July 13, 2014)

that they should not be classified come under the classification "RC" and comes under the category of prohibited content.

3.7.4 Brazil

The President of Brazil signed into law, Marco Civil da Internet[37], often dubbed as the Internet Bill of Rights, on April 23, 2014. The bill was drafted by a collaborative process involving general public and various organisations and this was seen as a model that could be followed by the rest of the world.

The legislation provides safe - harbour protection to intermediaries and requires intermediaries to take down content only on receipt of a court order. The only exception to this is when there is a breach of privacy arising from the disclosure of materials containing nudity or sexual activities of a private nature.

Art.18 of the legislation states that the provider of connection to Internet cannot be held to be liable for civil damages resulting from third-party generated content.

Art.19 further provides that provider of Internet application can only be subject to civil liability for damages resulting from third party content if, after a specific court order it does not take steps, to make unavailable the content identified as being unlawful. The court order must include clear identification of specific content identified as unlawful. For the purpose of identifying infringement of rights with respect to third party content, regard shall be given to freedom of speech and other rights guaranteed under Art 5 of the Brazilian Constitution.

...requires intermediaries to take down content only on receipt of a court order.

Art.21 provides that the Internet application provider that makes third party generated content available shall be held liable for the breach of privacy arising from the disclosure of images, videos and other materials containing nudity or sexual activities of a private nature, without the authorization of the participants, when, after receipt of notice by the participant or his/hers legal representative, refrains from removing, in a diligent manner, within its own technical limitations, such content. Wherever contact details of the user, directly responsible for content, are available with the provider of Internet applications, he shall have the obligation of informing the user about the execution of court order with information that allows the user to legally contest and submit a defense in court, unless otherwise provided by court order or law. In case of a take-down, the Internet application provider shall, when requested by the user whose content was made unavailable, replace the content with a note of explanation or the court order that gave grounds to the unavailability of such content.

[35] Australian Communications and Media Authority, *Prohibited Online Content*, *available at* http://www.acma.gov.au/Industry/Internet/Internet content/Internet-content-complaints/prohibited-online-contentinternet-safety-i-acma, (last visited July 13, 2014)

[36] National Classification Code, May 2005, *available at* http://www.comlaw.gov.au/Details/F2013C00006, (last visited July 13, 2014)

[37] Marco Da Civil, English translation, available at http://www.cgi.br/pagina/marco-civil-law-of-the-internet-inbrazil/180, (last visited July 13, 2014

3.7.5 Summary of take-down provisions in countries

Country	Classification of intermediaries	Safe harbour Protection	Take-down procedure	Put-back
Australia	**Copyright:** Category A (Mere conduit) Category B (Caching) Category C (Hosting) Category D (Location tool - links) **Prohibited Content:** Hosting service Live content service Links Service	Yes	Yes Yes	Yes No
Brazil	**Internet connection providers** **Internet application providers**	Yes	Yes	No
Canada	**Copyright:** Communications service Caching service Hosting Service	Yes	Yes	Yes
China	Conduits Caching service Hosting service Referral service	Yes	Yes	Yes
France	Mere conduits Hosting service Caching service	Yes	No	No
Germany	Mere access providers Hosting providers Caching providers	Yes	No	No
India	N/A	Yes	Yes	No
Japan	N/A	Yes	Yes	Yes
New Zealand	**Copyright:** Transmission service Routing service Connection service Hosting service **Other unlawful content:** N/A	Yes Yes	Yes No	No No
Republic of Korea	N/A	Yes	Yes	Yes

South Africa	Mere conduit Caching service Hosting service Information location tools	Yes	Yes	No
UK	**Copyright:** Mere conduit Hosting service Caching service **Defamatory content:** N/A	Yes Yes	Yes Yes	Yes Yes
USA	**Copyright:** Communication conduits Content hosts Search service Application service	Yes	Yes	Yes

Most of the countries above have a take-down regime only in the case of content that infringes on copyright. Defamation or other type of unlawful content can be taken down in most jurisdictions only by obtaining a court order. In the UK, although defamatory content can be sought to be taken down, there is a well defined notice and counter-notice mechanism to protect the rights of the content-creator.

4. Recommendations of the Lok Sabha Committee on Subordinate Legislation

The Intermediary Guidelines Rules were reviewed by the Lok Sabha Committee on Subordinate Legislation. The Committee considered the written submissions made by SFLC.IN, the Society for Knowledge Commons and the Centre for Internet & Society and also looked into the response to these submissions made by DEITY. The Committee also heard oral submissions made by SFLC.IN and the Society for Knowledge Commons and DEITY under the Ministry of Communications and Information Technology. The 31st Report of the Committee on Subordinate Legislation (2012-2013) was presented before the Lok Sabha on 21 March 2013 by Shri P Karunakaran, Chairman of the Committee.

A brief overview of the major issues raised and addressed may be found in the table below:

Issue raised	DEITY's response	LSCSL's recommendation	Action taken
Arbitrary and undefined terms featured in Rule	Impugned terms taken from existing legislations,	Definitions of terms used in different laws	Matter is *subjudice*; decision by

3(2)	judgments; they are common terms of international legal parlance; however, there is certainly room for improvement in terms of removal of ambiguity	should be incorporated at one place in the Rules; terms undefined by other statutes should be defined and incorporated into the Rules	courts awaited
Current taken-down procedure under Rule 3(4) facilitates precensorship, imposes unfair burden on intermediaries, confers adjudicatory role on intermediaries	Since take-down is not *mandatory* as per the Rules, there is no precensorship; intermediaries are only required to *initiate* action within 36 hours as per Rule 3(4) – Rule 3(11) gives them 30 days to actually take action; Rules have been framed in line with international practice	Take-down procedure should be clarified; there should be safeguards to protect against abuse during such process	Clarification issued by DEITY on 18/3/13 to the effect that intermediaries are only required to *initiate* action within 36 hours of notification, and take action within 30 days
CRAC not functional despite express provisions in the IT Act and Rules	CRAC has been reconstituted; meeting held on 29/11/12	CRAC should be made functional with members representing interests of those principally affected or having special knowledge of subject matter	CRAC reconstituted with members from Government, industry, academia, user association.

The first issue taken up for consideration was that Rule 3(2) of the Intermediaries Guidelines Rules employs several terms such as 'grossly harmful' and 'blasphemous' (among others), which in addition to being highly subjective and arbitrary, are not defined under the IT Act, Rules or any other legislation. In response, DEITY stated that the impugned terms were taken from existing Indian legislations such as the IPC and CrPC, and also from various judgments of the Courts, but have not been defined as such. However, they are common terms of international legal parlance, and Internet companies worldwide have used them in their Terms of Service with users. It was nevertheless admitted by DEITY that there certainly is room for improvement in the Intermediaries Guidelines Rules so that there is no ambiguity.

It was nevertheless admitted by the DEITY that there certainly is room for improvement in the Intermediaries Guidelines Rules so that there is no ambiguity.

The Committee then moved on to examine several issues regarding the disablement of information by intermediaries, where Rule 3(4) was alleged *inter alia* to facilitate pre-censorship, impose unfair burdens on intermediaries and endow an impractical adjudicatory role on intermediaries that they are not equipped to handle. In response, DEITY representatives stated that on obtaining knowledge of infringing content, Rule 3(4) requires intermediaries to act within 36 hours and wherever applicable, work with users/owners to disable such information that is in contraction of Rule 3(2). Rule 3(4) clearly says that intermediaries "shall act". The meaning of 'act' here is

merely that intermediaries should *initiate* and decide on a course of action within 36 hours. Rule 3(11) then provides intermediaries 30 days to actually deal with the matter. Due to the elements of on-line anonymity and lack of cooperation from international intermediaries, it is difficult at times to trace specific users who posted infringing content. It is then the responsibility of intermediaries who know and have details of users to work with them towards making decisions on disablement. In such a situation, the Ministry of Communications and Information Technology (MCIT) does not think the rule is violative of natural justice, and as it is not *mandatory* for intermediaries to disable information, the Rules do not lead to any kind of censorship. DEITY also emphasized the fact that the Rules were formulated in line with international practise, where intermediaries routinely entertain requests for disablement of information. All the Indian Intermediaries have implemented these Rules and have not raised any issue at any point of time.

DEITY representatives further demonstrated the need to retain Rule 3(4) by drawing the Committee's attention to transparency reports published by Indian intermediaries. While the number of disablement request from India have been considerably lower than in other countries like USA or Germany, only 30% of such requests are actually complied with. In light of the circumstances, Rule 3(4) provides a statutory compliance mechanism, where intermediaries are required to initiate action on disablement requests within 36 hours and take necessary action within 30 days. As noted by the Committee, this paints a somewhat conflicting picture in terms of legal enforceability of the Rules. While it was said in the context of censorship that the Rules are only of an advisory nature meant to promote self-regulation by intermediaries, they were described as statutory mandates while elaborating on the meaning of the term "shall act" within Rule 3(4).

Based on the written and oral submissions received, the Committee in its report directed as follows:

- In order to remove ambiguity in the minds of the people, the definition of those terms used in different laws should be incorporated at one place in the aforesaid Rules for convenience of reference by the intermediaries and general public. In regard to those terms which are not defined in any other statute, these should be defined and incorporated in the Rules to ensure that no new category of crimes or offences is created in the process of delegated legislation.
- There is need for clarity on the legal enforceability of the Rules. If need be, the position may be clarified in the Rules particularly on the process for take down of content and there should be safeguards to protect against any abuse during such process.
- The MCIT is urged to take such steps as deemed necessary to enlist the co-operation of international intermediaries.
- The Cyber Regulations Advisory Committee is to be made functional so that the MCIT may benefit from its advice particularly in the context of having a fresh look at the Rules and amendment of Rules recommended in this report. It should also be made clear if there are members representing the interests of those principally affected or having special knowledge of the subject matter as expressly stipulated in Section 88(2) of the IT Act.
- The MCIT is required to take urgent steps to ensure that Rules under Sections 70A(3) and 70B(3) of the IT Act (regarding the manner of performing functions and duties of "Critical Information Infrastructure Protection Agency"and terms and conditions of employees of "Indian Computer Emergency Response Team") are finalized and notified without any further delay.

In its 40th Report presented before the Lok Sabha on 19 February 2014, the Committee on Subordinate Legislation went over the actions taken by the Government towards implementing the Committee's recommendations from the 31st report. The following steps were taken pursuant to said recommendations:

- DEITY issued a clarification on 18.3.2013 according to which, the intended meaning of the words "shall act within thirty six hours" as mentioned in Rule 3(4) is that the intermediary shall respond or acknowledge to the complainants within 36 hours of receiving the complaints/grievances about any such information as mentioned in Rule 3(2) and initiate appropriate action as per law.
- The MCIT clarified that with regard to the issue of removal of malicious content on the websites hosted outside the country, wherever the requisite cooperation is not forthcoming from foreign intermediaries, Government has provision under Section 69A of the IT Act to block access to such objectionable content. As far as the issue of securing cooperation from foreign intermediaries in sharing information related to the user hosting objectionable contents on their websites, Government has initiated steps to enhance international cooperation to effectively deal with the issues of cyber crimes and cyber security.
- The MCIT submitted that the reconstituted Cyber Regulation Advisory Committee (CRAC), having members from Government including Law-enforcement agencies, academia (IITs), Industry Associations (NASSCOM, ISPAI, FICCI, ASSOCHAM) and user Association (Computer Society of India), is functional and its last meeting was held on 29.11.2012. In the said meeting, CRAC discussed the Rules notified under the IT Act and gave useful advice in this regard.

Regarding the definition of terms under the Rules, the MCIT submitted that the matter is *sub-judice* and a decision is awaited from the Courts. The Committee however noted that Rules under Sections 70A(3) and 70B(3) of the IT Act had still not been framed or notified despite the Committee's express directions, and advised the Government to ensure that this is done without further delay. Although CRAC is constituted, we find that the committee does not hold regular meetings and the discussions of the meetings are also not made public.

5. Motion to annul Information Technology (Intermediaries Guidelines) Rules, 2011

On 23rd March 2012, Mr. P Rajeeve, Member of Parliament moved a motion[38] in the Rajya Sabha to annul the Intermediaries Guidelines Rules on the following grounds:

- The Rules are *ultra vires* to the parent Act for the following reasons:
- As per Rule 3(4), intermediaries are required to disable access to content that falls under Rule3(2)(b) within 36 hours of being notified. Rule 3(2)(b), while specifying prohibited content, employs several terms such as 'grossly offensive' and 'blasphemous' that are undefined by the IT Act, Rules or any other legislation. In the absence of statutory definitions, intermediaries are forced to perform adjudicatory functions that they are not equipped to handle. This amounts to private censorship.

[38] Rajya Sabha List of Business, May 17, 2012, *available at* http://164.100.47.5/newlobsessions/sessionno/225/170512.pdf (last visited July 13, 2014)

- Rule 3(7) requires intermediaries to provide any information to authorized Government Agencies when asked to do so by lawful order. Said Rule does not specify any applicable procedure or safeguards for this purpose.
- The Rules were framed without seeking advice from the Cyber Regulations Advisory Committee, which has not even been constituted despite express provision to do so under Section 88 of the IT Act.

- The Rules are violative of Article 19 of the Constitution, since the prohibitions under Rule 3(2) exceed the purview of 'reasonable restrictions' on the Right to Freedom of Speech and Expression.
- The Rules do not allow users who had originally uploaded content in alleged contravention of Rule 3(2) to justify their cases before the content is to be taken down. This violates the principles of natural justice, and is highly arbitrary.
- The Rules prohibit the posting of certain content on the Internet, while the same may be permitted on other media such as newspapers or television.

Mr. Arun Jaitley – Leader of the Opposition – also spoke in support of issues raised by Mr. P Rajeeve. Taking stock of the underlying principle of free flow of information on the Internet, Mr. Jaitley observed with regard to Rule 3(2) that overly broad restrictions on the permissibility of online content would certainly constitute a threat to free speech. He raised specific objections to the use of the terms 'harmful', 'harassing', 'blasphemous', 'defamatory', 'libelous', 'disparaging', 'offensive', 'menacing', 'prevents the investigation of any offence' and 'insulting any other nation'. He therefore urged the reconsideration of the language used in Rule 3(2)[39].

> Mr. Jaitley observed with regard to Rule 3(2) that overly broad restrictions on the permissibility of on-line content would certainly constitute a threat to free speech.

Mr. Kapil Sibal, Hon'ble Minister for Communications & IT while replying to the motion, pointed out that the Internet is a new medium, which is capable of posing significant threats to national security and public safety. Since Indian laws do not apply *per se* on the Internet, there needs to be a mechanism to tackle such threats.

That said, the Minister insisted that the current legislative framework does not infringe on the rights of the media. He drew the Members' attention to Section 66 of the IT Act, which prescribes punishments for several substantive offences, and said that all Rules under the IT Act have been framed to aid its substance. He submitted that the argument that the Rules represent excessive delegation, has no substance.

Mr. Rajeeve's statement that the Intermediaries Guidelines Rules attempt to control cyberspace was taken up next for discussion. Here, the Minister emphasized the fact that the intermediaries' obligation to disable access to content is not absolute. On being notified of prohibited content, intermediaries may state in response that the impugned content is within limits prescribed by the Rules. The Government merely informs intermediaries that they bear obligations of due diligence under Section 79. It was said that the decisions on whether or not to disable access to content ultimately vests with the intermediaries themselves, and there is no Government interference in this regard. The Minister also

[39] The video of the speech by Mr.Arun Jaitley is available at http://www.youtube.com/watch?v=9La4zgCyviU

added that the intermediaries' obligation under Rule 3(4) to preserve content notified as unlawful for 90 days since being notified, was intended to aid the Government's investigative efforts. Immediate removal of notified content will have the effect of rendering further investigation into the matter impossible. It was also pointed out that Rule 3(4) requires intermediaries to 'work with the user or owner of allegedly unlawful content' on being notified, where applicable. This according to the Minister, offers ample opportunity to users who had originally uploaded the impugned content to justify their actions.

The Minister noted that every jurisdiction in the world has provisions similar to those being discussed. He felt that the Indian provisions are in fact more liberal than their international counterparts, including US and Europe. Further, the Rules were said to be consistent with the internal guidelines of intermediaries themselves. In support of his statement, the Minister cited the Yahoo! terms of use, which said 'You agree not to upload, post, email, transmit or otherwise make available any content that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful or racially, ethnically or otherwise objectionable'. Noting that these terms are far broader than those found in Rule 3(2), the Minister wondered why the Government's use of such terms are met with allegations of unconstitutionality while it is considered acceptable for intermediaries to employ similar terms.

One fails to understand how the complusion of pre censorship or imposition of adjudicatory roles on intermediaries might be justified by the 'nonbinding' nature of Rules.

In conclusion, the Minister invited Members of the House to write him letters detailing their objections to specific terms within the Rules, and promised to convene a meeting of Members, as well as the industry and all relevant stakeholders in order to arrive at a consensus and implement changes. Though the views expressed by the Minister do offer a cursory glance at the rationale of the Government behind notifying the Rules, one fails to understand how the compulsion of precensorship or imposition of adjudicatory roles on intermediaries might be justified by the 'nonbinding' nature of the Rules. Being notified under Sections 87(2)(zg) and 79(2) of the IT Act, the Intermediaries Guidelines Rules bear as much force of law as any other Rules similarly notified. To say then that the Rules are mere 'guidelines' that intermediaries are free to discard with no consequences, has no substance. Seeing how the applicability of safe harbour provisions laid down under Section 79 of the IT Act is contingent on the intermediaries' observance of 'due diligence' criteria spelt out by the Rules, misinformed decisions made by intermediaries to not take down contravening content may well result in their being held liable for said content.

Further, one must bear in mind that the use of broad and ambiguous terms in the Terms of Service of intermediaries is altogether different from their use in statutes. While the former is merely a contract of service between intermediaries and users, the latter is a legislative enactment by State, non-observance of which would be grounds for legal sanction. Hence, there is simply no room for ambiguity in statutes – a fact that should have received greater attention during the formative stages of the Intermediaries Guidelines Rules. Apart from reconsidering the broad language employed by Rule 3(2), the aforesaid issues of precensorship and conferment of adjudicatory roles on

intermediaries also need immediate attention from the Government. The lack of procedure and safeguards governing the invocation of Rule 3(7), which was left unaddressed by the Minister in his response to Mr. Rajeeve's motion, also needs to be taken up for further discussion. attention from the Government. The lack of procedure and safeguards governing the invocation of Rule 3(7), which was left unaddressed by the Minister in his response to Mr. Rajeeve's motion, also needs to be taken up for further discussion.

6. Reports and studies

6.1 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

The Human Rights Council in its resolution 7/36 requested the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression "to continue to provide his/her views, when appropriate, on the advantages and challenges of new information and communication technologies, including the Internet and mobile technologies, for the exercise of the right to freedom of opinion and expression, including the right to seek, receive and impart information and the relevance of a wide diversity of sources, as well as access to the information society for all". The report[40] submitted by Frank La Rue, dated May 16, 2011 looks into issues related to intermediary liability, censorship and privacy. The Special Rapporteur while commenting on the issue of intermediary liability has in this report stated that:

> While a notice and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors.

> *"41. Several States have sought to protect intermediaries through adopting variations on what is known as a "notice-and-takedown" regime. Such a system protects intermediaries from liability, provided that they take down unlawful material when they are made aware of its existence. For example, under the European Union-wide E-commerce Directive, a provider of hosting services for user-generated content can avoid liability for such content if it does not have actual knowledge of illegal activity and if it expeditiously removes the content in question when made aware of it. Similarly, the Digital Millennium Copyright Act of the United States of America also provides safe harbour for intermediaries, provided that they take down the content in question promptly after notification.*
>
> *42. However, while a notice-and-takedown system is one way to prevent intermediaries from actively engaging in or encouraging unlawful behaviour on their services, it is subject to abuse by both State and private actors. Users who are notified by the service provider that their content has been flagged as unlawful often have little recourse or few resources to challenge the takedown. Moreover, given that intermediaries may still be held financially or in some cases criminally liable if they do not remove content upon receipt of notification by users regarding unlawful content, they are inclined to err on*

[40] Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Agenda item 3, 17th Session of the Human Rights Council, May 16, 2011, *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (last visited July 13, 2014)

the side of safety by over-censoring potentially illegal content. Lack of transparency in the intermediaries' decision-making process also often obscures discriminatory practices or political pressure affecting the companies' decisions. Furthermore, intermediaries, as private entities, are not best placed to make the determination of whether a particular content is illegal, which requires careful balancing of competing interests and consideration of defences."

The Rapporteur while arguing against criminalisation of legitimate expression has said:

> *"Additionally, the Special Rapporteur reiterates that the right to freedom of expression includes expression of views and opinions that offend, shock or disturb. Moreover, as the Human Rights Council has also stated in its resolution 12/16, restrictions should never be applied, inter alia, to discussion of Government policies and political debate; reporting on human rights, Government activities and corruption in Government; engaging in election campaigns, peaceful demonstrations or political activities, including for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups"*

Thus, the report clearly argues against a take-down mechanism which offers little opportunity for the user to challenge a take-down of content. He has also cautioned against censoring opinions for the reason that it could be uncomfortable for a section of the society.

6.2 Study on Indian Online Intermediaries and the Liability System

This recently released study[41] was commissioned by the Global Network Initiative, a multistakeholder group of companies, civil society organizations, investors, and academics and was conducted by Copenhagen Economics, an economic consultancy. The study analysed the economic impact of online intermediaries in the Indian economy and the affect of the current legal regime on their businesses.

> The GDP contribution of online intermediaries may increase to more than 1.3 %($ 241 billion) by 2015, provided the current liability regime is improved.

Based on the methodology outlined in the OECD Digital Economy Paper, No.226 the study predicts that the GDP contribution of online intermediaries may increase to more than 1.3 %($ 241 billion) by 2015, provided the current liability regime is improved. Based on its research, the study states that the uncertain legal environment relating to intermediary liability poses a huge burden of costs and risks with virtually no benefits, which is likely to act as a barrier to the growth of Internet economy in India. To reach this conclusion, various companies, both home-grown ventures and firms that are a part of international groups, were taken into consideration during the study. Mouthshut.com, a first of its kind product review website in India, reveals that it receives over a 100 legal take down notices per month, and the company has appointed a team of five persons that solely works with issues surrounding the intermediary liability regime and handles complaints and legal notices from large businesses who have been reviewed, In another case study, Quikr, an e-commerce platform that allows sellers and buyers to post classified ads, reveals that the company maintains a team of 100 people, specifically dedicated to monitoring all user-generated content and searching for anything contentious which could expose the firm to the threat of litigation. Taking from Quikr's example,

[41] Martin Hvdit Thelle, Jan-Martin Wilk, Bruno Basalisco & Katrine Ellersgaard Nielsen, *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose*, Copenhagen Ecomonics, March 2014, *available at* http://globalnetworkinitiative.org/sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf (last visited April 1, 2014)

the study points out the issue of 'over-enforcement' by intermediaries as a result of the legal and regulatory environment that underpins the operation of online intermediaries in India. It reasons that because these intermediaries have to bear higher costs due to a high risk of being sued for third-party content, they choose to maintain a content-monitoring team to reduce the unjustified risk.

Another key consideration that the study takes into account is the heterogeneity in law enforcement across the country, again owing to uncertainty in the legal regime. Data reveals that Internet intermediaries, both established and start ups, across the country are faced with several litigation suits arising out of third party content. Interviews with these online intermediaries and legal experts reveal that there is a material degree of heterogeneity in how judiciary power and police enforcement are administered across the country. According to ebay India, lack of any judicial precedent and an unclear understanding of the law, has resulted in considerable variations in the enforcement of the IT Act across states. eBay India was sued by SSIL when counterfiet goods were listed on its websites, seeking that ebay monitor all content listed on its website. eBay opposed this on the grounds of impracticality to monitor all content and that it would lose its intermediary status and safeguard if it did so. In April 2013, the Supreme Court agreed with eBay's position and specified that, in case there were any further eBay listings of products affecting SSIL, it was the latter's responsibility to notify eBay. According to eBay India, the current liability regime creates a disadvantage for all intermediaries, even if the wider growth potential in India is fortunately a source of some attraction to developing entrepreneurships and investment in Internet businesses. eBay states thus, that Internet firms will still enter this space, yet it appears that the full potential of the Indian(Internet) economy is not being realised due to the constraints such as the liability rules applicable to online intermediaries.

The study concludes that the misguided level of protection surrounding intermediaries results in higher costs of doing business, which can only discourage a greater level of entrepreneurship and growth in this area.

6.3 Policy brief on Intermediary Liability developed by Article 19

Article 19, a civil society organisation that works for protection of Freedom of Expression of people across the world has come out with a policy brief[42] in the area of liability of Internet Intermediaries.

The key recommendations given are:

- Web hosting providers or hosts should in principle be immune from liability for third party content when they have not been involved in modifying the content in question.
- Privatised enforcement mechanisms should be abolished. Hosts should only be required to remove content following an order issued by an independent and impartial court or other adjudicatory body, which has determined that the material at issue is unlawful.
- From the hosts' perspective, orders issued by independent and impartial bodies provide a much greater degree of legal certainty.
- Notice-to-notice procedures should be developed as an alternative to notice and take down procedures. These would allow aggrieved parties to send a notice of complaint to the host. Notice-to-notice systems should meet a minimum set of requirements, including conditions

[42] Article 19, *Internet Intermediaries: Dilemma of Liability*, *available at* http://www.article19.org/data/files/Intermediaries_ENGLISH.pdf, (last visited June 2, 2014)

about the content of the notice and clear procedural guidelines that intermediaries should follow.

- Clear conditions should be set for content removal in cases of alleged serious criminality.

7. Feedback from Round-table discussions

In order to gather feedback from those principally affected by the Intermediaries Guidelines Rules as well as from the general public, SFLC.IN organized a series of Round Table Consultations in the following cities:

- New Delhi, Delhi (30th April 2013)
- Mumbai, Maharashtra (7th May 2013)
- Bangalore, Karnataka (10th May 2013)
- Cochin, Kerala (9th May 2013)

It was felt that New Delhi being the national administrative capital; Mumbai being the figurative commercial capital; Bangalore being the IT hub of India and Cochin being a small but bustling haven for small to medium businesses; this choice of cities would facilitate adequate and proportional participation from all principally affected quarters. Though members of the Government, industry, civil society etc. were specifically invited so as to ensure representation by all relevant stakeholders, participation in the event itself was open to all.

In the interest of keeping discussions streamlined and on-topic, the Consultations were centred around the following broad areas:

1. Explanation of safe harbour provisions under the Information Technology Act, 2000
2. Description of the procedure for take-down of third party content as laid down under the Information Technology (Intermediaries Guidelines) Rules, 2011
3. Discussion on the take-down mechanism and various take-down scenarios mentioned by the participants
4. Discussion on the guidelines proposed by SFLC.IN
5. Recommendations by the attendees on the procedure for removal of content
6. Eliciting responses to a Questionnaire on intermediary liability

Brief descriptions of the discussions at various venues are given below:

BANGALORE

The Bangalore round of Consultations were organised in partnership with the Indian Institute of Management, Bangalore. Issues raised here mostly concerned businesses and start-ups. The attendees suggested two mechanisms by which illegal third party content could be removed or disabled by intermediaries:

- Tripartite Redressal System
- Content-based Redressal System

Under the Tripartite Redressal System, resolution of complaints regarding content would involve three parties *i.e.* the content provider or third party, the complainant and the intermediary. The suggested procedure for removal of illegal content is as follows:

- The complainant will send 'Form 1', which provides details of alleged illegal content along with grounds for its removal, to the intermediary.
- The intermediary will then forward this complaint to the content provider i.e. the third party, along with a counter-complaint form.
- If the third party does not reply within a stipulated period of time, the content will be removed.
- If the third party submits a counter-complaint with adequate proof of legality of content and the complainant admits the proof, the content will be restored.
- If the parties do not agree with each other, the intermediary will discuss the content with the parties to come to a logical conclusion.
- If the parties are not able to reach a logical conclusion even after the discussion then they are free to approach any Court to decide upon the matter.

This would ensure that intermediary is not held liable for any action of or content provided by third parties.

Under the Content-based Redressal System, action taken by the intermediary would be based on the nature of the content created by the third party. The attendees suggested that:

- Any content which violates privacy of any individual or obscene or pornographic the content should be immediately removed.
- For content other than the above mentioned content, flagging mechanism could be adopted.
- In the flagging mechanism the complainant shall flag the content based on the nature of content. If the third party does not object to the flag by adducing proof of lawfulness of the content, then the material would be kept flagged. However, if the complainant wants removal of the content he should get a Court order to remove the content.

DELHI

The Delhi round-table had participants who were well aware of the issues and included policy heads from various Online Service Providers, representatives of industry bodies, civil society organisations and academia.

The attendees at Delhi raised objections based on the classification of intermediaries. The attendees were of the opinion that all the intermediaries cannot be treated alike. Most of the attendees felt that there is a need to classify the intermediaries based on the nature of service they are providing. Questions were further raised as to whether Business Process Outsourcing establishments could be categorised as an intermediary.

There was a view that it should not be made mandatory to provide the name of the complainant in Form1, which was suggested to be used for submitting a complaint. The attendees proposed that there should be an option for anonymous complainants. On the proposal of disclosure of notices received by the intermediaries, the representatives of intermediaries contested that such a rule would not be beneficial. However, after deliberation the attendees agreed that the intermediaries should disclose the actions taken by them after they have received notices for removal of content. The attendees further said that it would be a good industry practice. The attendees suggested that in case of defamatory content the complainant should get a Court order to remove the content. A mere notice

to the intermediary shall not suffice to remove the content.

Attendees of the Round Table consultation in Delhi also suggested creation of a separate body to decide upon matters pertaining to removal of content. It was also suggested that the intermediaries should publish transparency reports based on the complaints received from Government and private entities.

COCHIN

SFLC.IN did not want to restrict the consultations to big cities and the city of Cochin in Kerala was chosen to understand the experiences of small businesses and users. There was a good representation of users, with participation from the Wikipedia community, bloggers and free software community. The attendees representing intermediaries in the Round Table at Cochin shared their experience and the actions taken by them in such cases. They also raised various questions based on the classification of intermediaries and highlighted the problems with the current definition.

The attendees suggested two mechanisms for removal of content by intermediary. According to the first procedure, the content provided by the third party should be classified into two categories. The first category would consist of content which is:

- pornographic;
- considered as invasion of privacy of any individual;
- in accordance with reasonable restrictions under Article 19(2) of the Constitution of the India.

The other category should consist of content other than the above mentioned content.

In this mechanism the complainant shall forward Form 1 to the intermediary who is in control of the content. It should not be sent to any other intermediary other than the intermediary who is closest to the content or in control of the content. If the content belongs to the first category then the content should be removed immediately. In case the content has been wrongly classified then the third party could get a Court order to restore the content.

In case the content belongs to the second category then the content should be flagged and the flag should state the reason for such objection. The intermediary should wait for a counter notice from the content creator for a period of 5-7 days. If the content creator does not respond within the period then the content could be disabled. But the intermediary will have to wait for further 21 days to remove the content. If the content creator sends a counter-notice, the content will be restored. The complainant will have to get a court order to get the content removed.

A suggestion by the attendees from the Wikipedia community was for the creation of a discussion forum. They suggested that in case of any objection to the content, the decision would rest on the decision of the discussion forum. If the discussion forum is of the opinion that the content should be removed then the decision is binding on the intermediary and visa versa.

MUMBAI

There should be classification on the basis of content, user and intermediary.

Mumbai as the business capital saw participation in the round-table from businesses, journalists and civil society. The attendees to the Round Table at Mumbai suggested that there should be classification on the basis of content, user and intermediary. They suggested that at the initial level the content should also be classified on the basis of image, video and others. They also suggested that the users who are getting affected by the content should be classified as individual and corporate. Further, they also suggested that there should be a

classification for the urgency in removal of content. They should be classified as:

- immediate,
- urgent and
- time period more than 36 hrs.

The attendees proposed 3 mechanisms for removal of content.
The proposals are:

1. There should not be a take down procedure initiated based on a private complaint. If the content is harming anyone the affected person should approach the Court.
2. Flagging mechanism wherein
    - If any user is unhappy with the content then they should flag the content and wait for the content creator's response.
    - If the third party does not respond the content would be removed.
    - If he responds with evidence regarding the genuine nature of the content, the content is unflagged.
    - If they are not able to reach a conclusion then they should get a court order to get the content restored or removed.
3. Another proposal was for a moderator based system where the content has to be verified by the moderator. If the moderator is happy with the content then it should be published. If the volume of content is such that it could not be moderated then the second system should be followed.

Summary

The round-table discussions were very helpful in understanding the views of the users and the industry on the issue of intermediary liability and content take-down. The feedback of the discussions could be summarised as follows:

- Intermediaries should not be made to decide on the legality or otherwise of user generated content.
- The complainant has to procure a court order for a permanent take-down of content.
- Mechanisms like flagging of content could be adopted instead of take-down in case of complaints.
- Take-down should be resorted by the intermediaries only in cases where privacy of an Individual is breached by uploading of obscene content.
- In case of adoption of a take-down mechanism, there should be a put-back provision to enable the content-creator to respond to the complaint.

8. Principles for a take-down system

SFLC.IN proposes the following principles based on the consultations, our analysis of existing literature and reports, mechanisms adopted by various countries and, close and detailed interactions we had with industry, users, journalists, academia and other civil society organisations.

The basic premise of the regulation of online content should be that intermediaries that host user generated content should be granted protection from legal liability that arises from such content on their complying with the regulatory obligations. Such a protection is required for these media to serve as a platform for citizens to express their views openly and fearlessly and for these platforms to host such views without the fear of legal liabilities. We propose that the following principles may be considered in implementing any kind of "notice and action" system while respecting the process established by law, free expression and privacy of the users and ability of the industry to carry out its business:

The basic premise ofthe regulation ofonline content should be that intermediaries that host usergenerated content should be granted protection from legal liability that arises from such content on theircomplying with the regulatory obligations.

a) Restrictions should be clearly defined and only be imposed on content which is prohibited by the constitution.

b) There should be a provision of counter notice mechanism to the take-down notice.

c) There should be a put-back provision to restore the content if the complainant fails to obtain a court order within a stipulated time.

d) There should be clear guidance for Intermediaries about what is considered a valid notice and a standard form should be prescribed in the Rules for submitting a notice. There should be penalties for unjustified and frivolous notices.

e) The Courts should be the final authority to decide on the legality of content when the takedown request is opposed.

f) Intermediaries should not have an adjudicatory role in acting on take-down requests.

g) The intermediary should publish on their website a clear and easy to approach complaint redressal procedure.

h) There should be public disclosure by the intermediaries about notices received and actions taken.

i) Access to private information of users held by the intermediary should be provided only after complying with sufficient safeguards as mandated by the Supreme Court in *People's Union for Civil Liberties v. Union of India & Anr.*[43] on telephone tapping and statutes.

[43] (1997) 1 SCC 301

9. Conclusion

As technology evolves at a fast pace, the law should not be found wanting.

The Intermediaries Guidelines Rules in their current form are unconstitutional and administratively burdensome with no support of the user base. The authorities are well equipped by the IT Act to block any objectionable information in the interest of national security or public order, rendering private censorship efforts such as those embodied by the current Rules superfluous. In 2012, while urging the revision of the language of these Rules, Mr. Arun Jaitley, Union Minister of Finance and Defence, Government of India had aptly observed that overly broad restrictions on the permissibility of on-line content constitutes a threat to free speech. The Rules need to be amended by removing unconstitutional restrictions on free speech, adding a counter-notice and put-back provision so that the rights of content-creators are protected. The final decision on whether content is unlawful should be made by the judiciary. The provision for law enforcement agencies to access user-data should be removed from these Rules as such provisions exist in other statutes.

In India, the spread of mobile phone has been a truly revolutionary phenomenon and has made communication possible across the length and breadth of the country. The availability of Internet on mobile as the figures released by TRAI shows could be the driving factor for Internet adoption in the country. New models similar to CGNet Swara[44] could evolve making it easy for anyone, even the illiterate, to contribute content on the Internet. This could lead to greater transparency and accountability in governance and better access to knowledge.

As technology evolves at a fast pace, the law should not be found wanting. The law should be an enabling factor that ensures that citizens enjoy their right to freedom of speech and expression without any hindrance. India, being the largest democracy in the world should lead the world in ensuring that the citizens enjoy the right to express themselves freely online.

[44] CGNet Swara is a voice based portal that allows people to report stories of local interest and to listen to news. This has been successful in rural areas of Madhya Pradesh.

Annexure 1

The Information Technology (Intermediaries guidelines) Rules, 2011.

G.S.R (E).- In exercise of the powers conferred by clause (zg) of sub- section (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely: -

1. Short title and commencement.- (1) These rules may be called the Information Technology (Intermediaries guidelines) Rules, 2011.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions.- (1) In these rules, unless the context otherwise requires,- (a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Communication link" means a connection between a hypertext or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which could be another document or another website or graphical element.

(c) "Computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;

(d) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;

(g) "Indian Computer Emergency Response Team" means the Indian Computer Emergency Response Team appointed under sub section (1) of section 70(B) of the Act;

(h) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(i) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(j) "User" means any person who access or avail any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information or views and includes other persons jointly participating in using the computer resource of an intermediary.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Due diligence to be observed by intermediary.— The intermediary shall observe following due diligence while discharging his duties, namely : -

(1) The intermediary shall publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person.

(2) Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —

(a) belongs to another person and to which the user does not have any right to;

(b) is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

(c) harm minors in any way;

(d) infringes any patent, trademark, copyright or other proprietary rights;

(e) violates any law for the time being in force;

(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

(g) impersonate another person;

(h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.

(3) The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in sub-rule (2): provided that the following actions by an intermediary shall not amount to hosting, publishing, editing or storing of any such information as specified in sub-rule (2)-

(a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource;

(b) removal of access to any information, data or communication link by an intermediary after such information, data or communication link comes to the actual knowledge of a person authorised by the intermediary pursuant to any order or direction as per the provisions of the Act;

(4) The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any such information as mentioned in sub-rule (2) above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2). Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.

(5) The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy for access or usage of intermediary computer resource, the Intermediary has the right to immediately terminate the access or usage rights of the users to the computer resource of Intermediary and remove non-compliant information.

(6) The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

(7) When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative,protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

(8) The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011.

(9) The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

(10) The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act which may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force: provided that the intermediary may develop, produce, distribute or employ technological means for the sole purpose of performing the acts of securing the computer resource and information contained therein.

(11) The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rule 3 can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

[No. 11(3)/2011-CLFE]
(N. Ravi Shanker)
Joint Secretary to the Government of India

Annexure 2

Draft Rules circulated by SFLC.IN during the Round-table consultations

(These rules were circulated among the participants of the round-table consultations to gather feedback on suggestions related to the safe-harbour regime and take-down provisions. These were used as a framework for the discussions and to arrive at the principles that SFLC.IN has recommended in this report.)

The Information Technology (Intermediaries guidelines) Rules, 2013.

G.S.R (E).- In exercise of the powers conferred by clause (zg) of sub- section (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely: -

1. Short title and commencement.- (1) These rules may be called the Information Technology (Intermediaries guidelines) Rules, 2013.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions.- (1) In these rules, unless the context otherwise requires,□ (a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Communication link" means a connection between a hypertext or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which could be another document or another website or graphical element.

(c) "Complainant" means any person who is aggrieved by any information stored, hosted, published or linked to by an intermediary.

(d) "Computer resource" means computer resource as defined in clause (k) of sub-section (1) of section 2 of the Act;

(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Designated officer" means designated officer as defined in the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009;

(g) "Electronic Signature" means electronic signature as defined in clause (ta) of sub-section (1) of section 2 of the Act;

(h) "Form" means a form as appended to these rules;

(i) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(j) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

(k) "User" means any person who access or avail any computer resource of intermediary for the purpose of hosting, publishing, sharing, transacting, displaying or uploading information

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. **Due Diligence to be observed by intermediary: (1)**Intermediaries, whose service includes storing or hosting information or providing automated links or cache, shall follow the following due diligence while discharging their duties:

(a) The intermediary shall prominently display and publish rules and regulations, a privacy policy and terms of service for access or usage of the intermediary's computer resource by any person.

(b) Such rules and regulations shall inform the users of the complaint redressal mechanism as implemented by the intermediary.

(c) The intermediary shall prominently publish and display the name, address, phone number and electronic mail address of a Grievance Officer to whom a complaint under Rule 4 is to be made.

(d) On receipt of a complaint under Rule 4 , the Grievance Officer shall follow the complaint redressal mechanism as provided in Rule 5.

(2) Intermediaries, other than those covered by sub-rule (1), shall follow the following due diligence while discharging their duties:

The intermediary shall prominently display and publish rules and regulations, a privacy policy and terms of service for access or usage of the intermediary's computer resource by any person.

(3) Notwithstanding anything contained in sub rules (1) and (2), an intermediary is under no general obligation to monitor its services for seeking facts indicating illegal activity

4. **Complaint about unlawful act:** (1) Any person who is aggrieved by any information being hosted by an intermediary, that violates any law for the time being in force, shall submit a complaint with the Grievance Officer.

(2) Any complaint under sub-rule (1) shall be made in Form 1 and shall be in writing or through email signed with electronic signature.

(3) Complaint under sub-rule (1) shall be made only against intermediaries whose service, as regards the information about which complaint is made, includes storing or hosting the information or providing automated links or cache.

5. Grievance redressal: (1) The following procedure shall be followed on receipt of a complaint under Rule 4 by any intermediary that stores, hosts or publishes information:

(a) On receipt of a complaint as provided in Form I , the intermediary shall disable access to the alleged illegal information within forty eight hours and post a message at the site of the information clearly and prominently stating that access to the information has been disabled based on a complaint. The intermediary shall also clearly display a link to a counter complaint form and a page providing information about the process to be followed for filing a counter complaint.

(b) An aggrieved user desirous of contesting a complaint can prefer a counter complaint in the form and manner laid out in Form II in writing or through email with electronic signature.

(c) On receipt of the counter-complaint from the user, the intermediary shall furnish a copy of it to the complainant within 48 hours and also inform the complainant that the information will be restored if he does not furnish an order from a competent court as specified in clause (d).

(d) If the complainant fails to furnish an order from a court of competent jurisdiction ordering

the removal of the information complained of, within twenty one days of receiving a counter-complaint, the intermediary shall restore access to the information.

(2) Any intermediary that provides automatic communication links or intermediate and temporary storage of information, on receipt of a complaint under Rule 4 shall initiate action within 48 hours of receipt of such complaint to remove such communication links or to disable access to the information it has stored, if the information at the initial source of the transmission or the linked information has been removed from the network, or access to it has been disabled .

6. The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.

7. When required by a lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance.

8. The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011.

9. The intermediary shall report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team.

FORM 1

[*See* rule 4(2)]

A. Complaint

1) Name of the complainant.....
2) Address.....
3) City .....Pin Code.....
4) Telephone.....(Prefix STD Code)
5) Fax(if any).....
6) Email(if any).....

B. Details of offending information

1. URL/ web address of the information .....
(Please attach screen-shot/printout of the offending information)
2. Name of the Intermediary hosting the information .....
3. URL of the Intermediary.....
4. Reason for requesting disabling of access (Please tick):
i. Court Order: Details and attachment
ii. Interest of sovereignty or Integrity of India.
iii. Defence of India.
iv. Security of the state.
v. Friendly relations with foreign States.
vi. Public order
vii. For preventing incitement to the commission of any cognizable offence relating to above.
viii. Defamation
ix. Copyright infringement
x. Obscenity
xi. Other.....
5. Please state how the complainant is aggrieved by the information/ has a direct interest
.....
.....

C. Enclosures / Attachments:

1.
2.
3.

I/We solemnly swear and affirm that the facts and matters stated herein are true to the best of my/our knowledge, information and belief and that I/We am/are aggrieved by the offending information hosted by the intermediary.

Date ..... Place .....

Signature
(physical or electronic)

To
The Grievance Officer
(Name and address of the Intermediary)

FORM 2

[*See* rule 5(1)(b)]

A. Counter - complaint

1. Name of the user.....
2. Address.....
3. City .....Pin Code.....
4. Telephone.....(Prefix STD Code)
5. Fax(if any).....
6. Email .....
7. User-name /alias used to access the resource of the intermediary.....

B. Details of complaint

1. URL/ web address of the information .....
2. Name of the Intermediary hosting the information .....
3. URL of the Intermediary.....
4. Name of the complainant.....
5. Date of receipt of complaint .....

B. Grounds for countering the complaint:

Please state the grounds for countering the complaint:

.....

.....

C. Enclosures / Attachments:

1.
2.
3.

I/We solemnly swear and affirm that the facts and matters stated herein are true to the best of my/our knowledge, information and belief.

Date ..... Place .....

Signature

To

The Grievance Officer

(Name and address of the Intermediary)

ABOUT SFLC.IN

SFLC.IN is a donor supported legal services organisation that brings together lawyers, policy analysts, technologists, and students to protect freedom in the digital world. SFLC.IN promotes innovation and open access to knowledge by helping developers make great Free and Open Source Software, protect privacy and civil liberties for citizens in the digital world by educating and providing free and 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 get more information about protecting your rights in the online world.

K-9, Birbal Road, Second Floor,
Jangpura Extension
New Delhi-110014, India
Tel: +91-11-43587126
Fax: +91-11-24323530
www.sflc.in

This work is licensed under a Creative Commons
Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) License.

Time-line of Software Patent Law in India

June 25 2002	Section 3(k) introduced in the Patents Act,1970. Excludes mathematical, business methods, computer program per se or algorithms from patent protection.
December 26 2004	Patent (Amendment) Ordinance 2004 amends Section 3(k) to extend patentability to "Computer programmes having technical application to industry or in combination with hardware"
January 1 2005	2004 Ordinance comes into force.
March 18 2005	Patent (Amendment) Bill 2005 introduced in Lok Sabha still intact with the 2004 Ordinance amendment.
March 22 2005	Press release by Ministry of Commerce proposes to omit the changes introduced by the 2004 Ordinance for the reason that these may give rise to monopoly of multinationals.
March 23 2005	Opposition raised in Parliament to amendment proposed by Patent (Amendment) Bill 2005 to Section 3(k), as it was feared that the amendment would give rise to monopolies by multinationals.
April 4 2005	The Patents (Amendment) Act, 2005 repeals the 2004 Ordinance. Patents Act 1970 restored to its original form.
March 2008	*'Draft Manual of Patent Practice and Procedure'* released by the Indian Patent Office(IPO). States "Claims directed to technical process, which is carried out under the control of a computer programme (whether by hardware or software) cannot be regarded as relating to computer programmes as such....Claims relating to software programme products are nothing but computer programmes per se simply expressed on computer readable medium and not allowable."
October 24 2008	Report of the Parliamentary Standing Committee on Commerce presented before Rajya Sabha emphasizes the need to clearly define the words *'per se'* in Section 3(k).
March 22 2011	Modified *'Manual of Patent Office Practice & Procedure'* released by IPO. States "Mathematical methods, business methods and algorithms claimed in any form, are not patentable....If the claims, inter alia, contain subject matter which is not computer programme, it is to be examined

	whether such subject matter is sufficiently disclosed in the specification and forms an essential part of invention."
June 28 2013	Draft Guidelines for Computer Related Inventions 2013 released by IPO. New term i.e. technical effect introduced in the Draft Guidelines with the purpose to explain 'technical advancement' under the Patents Act 1970. Draft Guidelines clarify that business methods, mathematical methods and algorithms cannot be patented irrespective of language used. Comments invited on the draft guidelines.
October 11 2013	Stakeholder Consultation organized by IPO. SFLC.in participated in the consultation and submitted additional comments.
December 19 2014	Draft of National IPR Policy released for public consultation. Proposes to "engage actively in negotiation of international treaties and agreements; to examine accession to some multi-lateral treaties which are in India's interest; and, become signatory to those treaties which India has de facto implemented to enable it to participate in their decision making process."
August 21 2015	Guidelines for Examination of Computer Related Inventions released by IPO. Provide that: - Mere use of mathematical formula in a claim to clearly specify the scope of protection being sought would not render the claim a mathematical method. Eg. Method of encoding, decoding, encryption - While business methods are non-patentable, if the claimed matter specifies an apparatus or technical process for carrying out invention even in part, the claims to be examined as whole - So long as a computer programme is not claimed in itself, but in a manner so as to establish industrial applicability and fulfils all other criteria of patentability, the patent should not be denied.
September 15 2015	SFLC.in writes a joint letter to Prime Minister of India expressing concern over the 2015 Guidelines for Examination of Computer Related Inventions.
September 21 2015	In response to the joint representation, Department of Industrial Policy &

Promotion, Ministry of Commerce, writes to Controller General of Patents with a request to examine the 2015 Guidelines and take appropriate action in the matter.

F. No. 1(3)/2014 – EG II

Ministry of Communication & Information Technology

Department of Electronics & Information Technology

POLICY

Title of Policy: **"Policy on Adoption of Open Source Software for Government of India"**

Preamble

Government of India (GoI) is implementing the Digital India programme as an umbrella programme to prepare India for a knowledge based transformation into a digitally empowered society and a knowledge economy. Under the overarching vision of Digital India, GoI aims to make Government services digitally accessible to citizens in their localities and to ensure efficiency, transparency and reliability of such services at affordable costs. To meet this objective, there is a need to set up a commensurate hardware and software infrastructure, which may require significant resources.

Organizations worldwide have adopted innovative alternative solutions in order to optimise costs by exploring avenues of "Open Source Software". GoI has also been promoting the use of open source technologies in the e-Governance domain within the country in order to leverage economic and strategic beneifts.

Further, the National Policy on Information Technology, 2012 has mentioned, as one of its objectives, to "Adopt open standards and promote open source and open technologies".

In view of the above, there is a need to formulate a policy for the Government Organizations to adopt Open Source Software. The "Policy on Adoption of Open Source Software for Government of India" (hereinafter referred to as "Policy") will encourage the formal adoption and use of Open Source Software (OSS) in Government Organizations.

1. Objectives

- To provide a policy framework for rapid and effective adoption of OSS
- To ensure strategic control in e-Governance applications and systems from a long-term perspective.
- To reduce the Total Cost of Ownership (TCO) of projects.

2. Definitions

Refer Glossary (Page No. 7)

3. Policy Statement

Government of India shall endeavour to adopt Open Source Software in all e-Governance systems implemented by various Government organizations, as a preferred option in comparison to Closed Source Software (CSS).

The Open Source Software shall have the following characteristics:

3.1 The source code shall be available for the community / adopter / end-user to study and modify the software and to redistribute copies of either the original or modified software.

3.2 Source code shall be free from any royalty.

4. Nature of Compliance

Mandatory

5. Applicability

The policy shall be applicable to all Government Organisations under the Central Governments and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

6. How to comply

All Government Organizations, while implementing e-Governance applications and systems must include a specific requirement in Request for Proposal (RFP) for all suppliers to consider OSS along with CSS while responding. Suppliers shall provide justification for exclusion of OSS in their response, as the case may be. Government Organizations shall ensure compliance with this requirement and decide by comparing both OSS and CSS options with respect to capability, strategic control, scalability, security, life-time costs and support requirements.

7. Exception

GoI shall endeavour to adopt Open Source Software in all e-Governance applications and systems implemented by Government Organizations. However, in certain specialised domains where OSS solutions meeting essential functional requirements may not be available or in case of urgent / strategic need to deploy CSS based solutions or lack of expertise (skill set) in identified technologies, the concerned Government Organization may consider exceptions, with sufficient justification.

8. Implementation Mechanism

i) GoI shall publish a policy framework for rapid and effective adoption of OSS covering the prioritization of the application areas and illustrative list of OSS & OSS Stacks etc, required for various functional areas.

ii) All future Requests for Proposals (RFPs) of e-Governance projects shall include a mandatory clause for considering Open Source Software (OSS) as a preferred option in comparison to Closed Source Software (CSS). Suppliers shall provide justification for exclusion of OSS in their response.

iii) Government Organizations shall ensure compliance with this requirement and decide by comparing both OSS and CSS options with respect to capability, strategic control, scalability, security, life-time costs and support requirements.

iv) GoI shall establish suitable support mechanism for the available OSS that includes Institutional Mechanism, Partnership with Industry, Academia and OSS Community.

v) GoI shall actively collaborate with OSS communities in India as well as at the International level and contribute wherever appropriate.

9. Review of the Policy

GoI shall have the right to review the Policy as and when required.

10. Point of Contact

All queries or comments related to the "Policy on Adoption of Open Source Software for Government of India" shall be directed to JS (e-Governance), DeitY (jsegov@deity.gov.in).

GLOSSARY

Definitions

1 **Domain:** A sub-category under an Information Technology field is a Domain; specific purpose within a "Domain" is known as "Area". For example, "Document type for Web publishing content" is one Area under the "Presentation" domain.

2 **e-Governance:** A procedural approach in which the Government and the citizens, businesses, and other stakeholders are able to transact all or part of activities using Information and Communication Technology tools.

3 **Government Organization:** For the purpose of this policy, Government organisation refers to all Ministries/ Departments/ offices/ statutory bodies/ autonomous bodies, both at the Central and State levels. Government organizations offering commercial services are not included.

4 **Legacy System:** An old method, technology, computer system, or application program that continues to be used, typically because it still functions for the users' needs, even though newer technology or more efficient methods of performing a task are now available.

5 **New version of Legacy System:** The legacy system which has undergone a major version change due to re-engineering like functional changes, architectural changes, technology changes,

change in storage mechanism, design implementation changes etc.

6 **Open Source Software:** OSS is commonly known as Free and Open Source Software (FOSS). Here the "Free" refers to "Freedom to use" and not "Free of Charge". Here "Open Source" refers to the "availability of Source code for the community / adopter / end-user to study and modify the software and to redistribute copies of either the original or modified software (without having to pay royalties to previous developers).

7 **Proprietary Software/ Closed Source Software:** CSS/proprietary software typically prohibits the access to / modification of the source code. It restricts the copy, modification, distribution and reuse of the software. The restrictions may be applicable to the whole or part of the software so that the control is with the concerned company. Revenue, profit and IPR drive the development and marketing of the products and solutions.

8 **Royalty:** A stream of payments for use of a certain type of asset/technology, most typically an Intellectual Property Right (IPR).

9 **Systems:** A group of interacting, interrelated, or interdependent elements forming a complex whole. Information System is a combination of people, hardware, software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose.

Non-Profit Organizations – Free Software Fiscal Sponsorship and Administrative Collaboration; New Ideas in 501(c)(3) Creation

Software Freedom Law Center
October 30, 2015

Free Software Fiscal Sponsorship and Administrative Collaboration:

1) Apache Software Foundation: How It Works

2) Free Software Support Network: Our Services

3) Software Freedom Conservancy: Applying

4) Software Freedom Conservancy: Member Project Services

5) Software in the Public Interest: Associated Projects HowTo

6) Software in the Public Interest: Relationship Between SPI and Associated Projects

7) Software in the Public Interest: Services Offered to Associated Projects

New Ideas in 501(c)(3) Creation:

1) Department of the Treasury, Internal Revenue Service: New 1023-EZ Form Makes Applying for 501(c)(3) Tax-Exempt Status Easier; Most Charities Qualify

2) Department of the Treasury, Internal Revenue Service: Instructions for Form 1023-EZ

3) Department of the Treasury, Internal Revenue Service: Form 1023-EZ

How the ASF Works

Available from: https://www.apache.org/foundation/how-it-works.html

This page will give you an overview of everything you always wanted to know about the Apache Software Foundation but were afraid to ask. The difference between membership and committership, who decides what, how elections take place, how is our infrastructure setup, what is the board, what is a PMC, what's the philosophy behind the incubator, and how the ASF is dealing with the incredible growth in new projects and contributors over the years. Come and see behind the scenes of the ASF.

- What is the Apache Software Foundation?
- A bit of history
- Meritocracy
- The Foundation structure
- Roles
- Project management
- The Foundation Infrastructure
- The Foundation Incubator
- Other Foundation entities
- Conclusions

What is the Apache Software Foundation?

The Apache Software Foundation (ASF) is a 501(c)3 non-profit public charity organization incorporated in the United States of America and was formed in 1999 primarily to:

- provide a foundation for open, collaborative software development projects by supplying hardware, communication, and business infrastructure

- create an independent legal entity to which companies and individuals can donate resources and be assured that those resources will be used for the public benefit
- provide a means for individual volunteers to be sheltered from legal suits directed at the Foundation's projects
- protect the 'Apache' brand, as applied to its software products, from being abused by other organizations

That's the dry fact, but how did all this come to be and what does it really mean in its details? We need to step back a little in history.

A bit of history

The foundation was created in 1999 by a group of people, that called themselves the "Apache Group" and had come together several years earlier, to continue to support and maintain the HTTPD web server written by the NCSA.

That server was freely available, came with source code and was licensed under a license that allowed very open modification and redistribution, but the original developers lost interest in that project and moved onto something else, leaving users with no support.

Some of those users started to exchange fixes (called "patches") and information on how to prevent problems and improve the existing software. Brian Behlendorf created a mailing list on his own machine for those users to collaborate to fix, maintain and improve that software.

The name 'Apache' was chosen from respect for the Native American Apache Nation, well-known for their superior skills in warfare strategy and their inexhaustible endurance. It also makes a cute pun on "a patchy web server" -- a server made from a series of patches -- but this was not its origin. The group of developers who released this new software soon started to call themselves the "Apache Group".

Between 1995 and 1999, the Apache HTTPD Web Server created by the Apache Group became the leader of the market (and currently still is, with more than 65% of the web sites in the world powered by it).

But as the web grew bigger, economical interests started to grow, and the Apache web site hosted new sister projects (such as the mod_ perl project, the PHP project, the Java Apache project). The need for a more coherent and structured organization that would shield individuals from potential legal attacks felt more and more necessary.

You can read more about ASF History.

Meritocracy

Unlike other software development efforts done under an open source license, the Apache Web Server

was not initiated by a single developer (for example, like the Linux Kernel, or the Perl/Python languages), but started as a diverse group of people that shared common interests and got to know each other by exchanging information, fixes and suggestions.

As the group started to develop their own version of the software, moving away from the NCSA version, more people were attracted and started to help out, first by sending little patches, or suggestions, or replying to email on the mail list, later by more important contributions.

When the group felt that the person had "earned" the merit to be part of the development community, they granted direct access to the code repository, thus increasing the group and increasing the ability of the group to develop the program, and to maintain and develop it more effectively.

We call this basic principle "meritocracy": literally, government by merit.

What is interesting to note is that the process scaled very well without creating friction, because unlike in other situations where power is a scarce and conservative resource, in the Apache group newcomers were seen as volunteers that wanted to help, rather than people that wanted to steal a position.

Being no conservative resource at stake (money, energy, time), the group was happy to have new people coming in and help, they were only filtering the people that they believed committed enough for the task and matched the human attitudes required to work well with others, especially in disagreement.

After explaining the structure of the ASF, we will see how the meritocracy relates to the various roles.

The Foundation structure

As the Apache Web Server started to grow in market share and popularity, due to synergy of its technical merit and to the openness of the community behind the project, people started to create satellite projects. Influenced by the spirit of the community they were used to, they adopted the same traditions of community management.

So, by the time the ASF was created, there were several separate communities, each focused on a different side of the "web serving" problem, but all united by a common set of goals and a respected set of cultural traditions in both etiquette and process.

These separate communities were referred to as "projects" and while similar, each of them exhibited little differences that made them special.

In order to reduce friction and allow for diversity to emerge, rather than forcing a monoculture from the top, the projects are designated the central decision-making organizations of the Apache world. Each project is delegated authority over development of its software, and is given a great deal of latitude in designing its own technical charter and its own governing rules.

At the same time, the cultural influence of the original Apache group was strong and the similarities between the various communities are evident, as we'll see later.

The foundation is governed by the following entities:

- Board of Directors (board) governs the foundation and is composed of members.
- Project Management Committees (PMC) govern the projects, and they are composed of committers. (Note that every member is, by definition, also a committer.)
- Various Officers of the corporation, appointed by the board, who set Foundation-wide policies in specific areas (legal, brand, fundraising, etc.)

For all the details, read our Governance overview.

Board of Directors (board)

The board is responsible for management and oversight of the business and affairs of the corporation in accordance with the foundation Bylaws. This includes management of the corporate assets (funds, intellectual property, trademarks, and support equipment) and allocation of corporate resources to projects.

However, technical decision-making authority regarding the content and direction of the Apache projects is assigned to each respective project management committee.

The board is currently composed by nine individuals, elected between the members of the foundation. The bylaws don't specify the number of officers that the board should have, but historically, this was the number of the first board and it has never changed. The board is elected every year.

The board website has more information, the list of the current directors, schedule of meetings, and past minutes.

Project Management Committees (PMC)

The Project Management Committees are established by resolution of the Board, to be responsible for the active management of one or more communities, which are also identified by resolution of the Board.

Each PMC consists of at least one officer of the ASF, who shall be designated chairperson, and may include one or more other members of the ASF.

The chair of the PMC is appointed by the Board and is an officer of the ASF (Vice President). The chair has primary responsibility to the Board, and has the power to establish rules and procedures for the day to day management of the communities for which the PMC is responsible, including the composition of the PMC itself. See further discussion about the role of PMC chair and why chairs are officers.

The ASF Bylaws (section 6.3) define a PMC and the position of chair. Some other emails help to clarify: here and here.

The role of the PMC from a Foundation perspective is oversight. The main role of the PMC is not code and not coding - but to ensure that all legal issues are addressed, that procedure is followed, and that each and every release is the product of the community as a whole. That is key to our litigation protection mechanisms.

Secondly the role of the PMC is to further the long term development and health of the community as a whole, and to ensure that balanced and wide scale peer review and collaboration does happen. Within the ASF we worry about any community which centers around a few individuals who are working virtually uncontested. We believe that this is detrimental to quality, stability, and robustness of both code and long term social structures.

We firmly believe in hats. Your role at the ASF is one assigned to you personally, and is bestowed on you by your peers. It is not tied to your job or current employer or company.

However those on the PMC are kept to a higher standard. As the PMC, and the chair in particular, are eyes and ears of the ASF Board, it is you that we rely on and need to trust to provide legal oversight.

The board has the faculty to terminate a PMC at any time by resolution.

The Apache Developer Information pages have many more details of how PMCs work. A complete list of all Apache projects is also available.

Officers

The Officers of the Apache Software Foundation oversee the day-to-day affairs of the Foundation. The officers are elected by the Board of Directors.

Roles

The meritocracy typically has various roles within each individual Apache project communities:

`user` **developer** **committer**

User

A ***user*** is someone that uses our software. They contribute to the Apache projects by providing feedback to developers in the form of bug reports and feature suggestions. Users participate in the Apache community by helping other users on mailing lists and user support forums.

Developer

A ***developer*** is a user who contributes to a project in the form of code or documentation. They take extra steps to participate in a project, are active on the developer mailing list, participate in discussions, provide patches, documentation, suggestions, and criticism. Developers are also known as ***contributors***

Committer

A ***committer*** is a developer that was given write access to the code repository and has a signed Contributor License Agreement (CLA) on file. They have an apache.org mail address. Not needing to depend on other people for the patches, they are actually making short-term decisions for the project. The PMC can (even tacitly) agree and approve it into permanency, or they can reject it. Remember that the PMC makes the decisions, not the individual committers.

PMC Member

A ***PMC member*** is a developer or a committer that was elected due to merit for the evolution of the project and demonstration of commitment. They have write access to the code repository, an apache.org mail address, the right to vote for the community-related decisions and the right to propose an active user for committership. The PMC as a whole is the entity that controls the project, nobody else. In particular, the PMC must vote on any formal release of their project's software products.

PMC Chair

The ***Chair*** of a Project Management Committee (PMC) is appointed by the Board from the PMC Members. The PMC as a whole is the entity that controls and leads the project. The Chair is the interface between the Board and the Project. PMC Chairs have specific duties.

ASF Member

An ***ASF member*** is a person who was nominated by current members and elected due to merit for the evolution and progress of the foundation. Members care for the ASF itself. This is usually demonstrated through the roots of project-related and cross-project activities. Legally, a member is a "shareholder" of the foundation, one of the owners. They have the right to elect the board, to stand as a candidate for the board election and to propose a committer for membership. They also have the right to propose a new project for incubation (we'll see later what this means). The members coordinate their activities through their mailing list and through their annual meeting. We have a full listing of Apache Members.

Project Management and Collaboration

The Apache projects are managed using a collaborative, consensus-based process. We do not have a hierarchical structure. Rather, different groups of contributors have different rights and responsibilities in the organization.

Since the appointed Project Management Committees have the power to create their own self-governing rules, there is no single vision on how PMCs should run a project and the communities they host.

At the same time, while there are some differences, there are a number of similarities shared by all the projects:

Communication

Communication is done via mailing lists. These identify "virtual meeting rooms" where conversations happen asynchronously, which is a general requirement for groups that are so geographically distributed to cover all time zones (like it's normally the case for the various Apache communities).

Some projects additionally use more synchronous messaging (for example, IRC or instant messaging).

Voice communication is extremely rare, normally because of costs and the language barrier (speech is harder to understand than written text).

In general, asynchronous communication is much more important because it allows archives to be created and it's more tolerant on the volunteer nature of the various communities.

Documentation

Each project is responsible for its own project website. Further information to assist committers, developers, and PMCs is available at ASF Infrastructure.

Decision Making

Projects are normally auto governing and driven by the people who volunteer for the job. This is sometimes referred to as "do-ocracy" -- power of those who do. This functions well for most cases.

When coordination is required, decisions are taken with a lazy consensus approach: a few positive votes with no negative vote is enough to get going.

Voting is done with numbers:

- +1 -- a positive vote
- 0 -- abstain, have no opinion
- -1 -- a negative vote

The rules require that a negative vote includes an alternative proposal or a detailed explanation of the reasons for the negative vote.

The community then tries to gather consensus on an alternative proposal that resolves the issue. In the great majority of cases, the concerns leading to the negative vote can be addressed.

This process is called "consensus gathering" and we consider it a very important indication of a healthy community.

Specific cases have some more detailed voting rules.

Philosophy

While there is not an official list, these six principles have been cited as the core beliefs of philosophy behind the foundation, which is normally referred to as "The Apache Way":

- collaborative software development
- commercial-friendly standard license
- consistently high quality software
- respectful, honest, technical-based interaction

- faithful implementation of standards
- security as a mandatory feature

All of the ASF projects share these principles. Similarly, Apache projects are required to govern themselves independently of undue commercial influence.

Operation

All projects are composed of volunteers and nobody (not even members or officers) are paid directly by the foundation for their job. There are many examples of committers that are paid to work on the projects, but never by the foundation themselves, but rather by companies or institutions that use the software and want to enhance it or maintain it.

Note that the ASF does contract out various services, including accounting, Press and Media relations, and infrastructure system administration.

Individuals compose the ASF

All of the ASF including the board, the other officers, the committers, and the members, are participating as individuals. That is one strength of the ASF, affiliations do not cloud the personal contributions.

Unless they specifically state otherwise, whatever they post on any mailing list is done *as themselves*. It is the individual point-of-view, wearing their personal hat and not as a mouthpiece for whatever company happens to be signing their paychecks right now, and not even as a director of the ASF.

All of those ASF people implicitly have multiple hats, especially the Board, the other officers, and the PMC chairs. They sometimes need to talk about a matter of policy, so to avoid appearing to be expressing a personal opinion, they will state that they are talking in their special capacity. However, most of the time this is not necessary, personal opinions work well.

Some people declare their hats by using a special footer to their email, others enclose their statements in special quotation marks, others use their apache.org email address when otherwise they would use their personal one. This latter method is not reliable, as many people use their apache.org address all of the time.

Balancing confidentiality and public discussion

We endeavour to conduct as much discussion in public as possible. This encourages openness, provides a public record, and stimulates the broader community.

However sometimes internal private mail lists are necessary. You must never divulge such information in public without the express permission of the list. Also never copy an email between private and public lists (no Cc). Such an event would go beyond the normal need for email ettiquette and be a serious breach of confidence. It could have serious ramifications, cause unnecessary confusion and ill-informed discussion.

Private lists are typically only used for matters pertaining to people as individuals (like voting in new committers), and legal matters that require confidentiality.

The Foundation Incubator

In order for new projects to be created, the ASF created a project called Incubator which is responsible to help new efforts to join the foundation.

Since the meritocratic rules operate across the ASF from bottom to top, it is vital for the long-term stability of such a form of government, that the initial set of committers has to know very well the dynamics of such a system, as well as share the same philosophical attitude toward collaboration and openness that the ASF expects from its projects.

The incubator is responsible for:

- filtering the proposals about the creation of a new project or sub-project
- help the creation of the project and the infrastructure that it needs to operate
- supervise and mentor the incubated community in order for them to reach an open meritocratic environment
- evaluate the maturity of the incubated project, either promoting it to official project/ sub-project status or by retiring it, in case of failure.

It must be noted that the incubator (just like the board) does not perform filtering on the basis of technical issues. This is because the foundation respects and suggests variety of technical approaches. It doesn't fear innovation or even internal confrontation between projects which overlap in functionality.

The incubator filters projects on the basis of the likeliness of them becoming successful meritocratic communities. The basic requirements for incubation are:

- a working codebase -- over the years and after several failures, the foundation came to understand that without an initial working codebase, it is generally hard to bootstrap a community. This is because merit is not well recognized by developers without a working codebase. Also, the friction that is developed during the initial design stage is likely to fragment the community.
- the intention to donate copyright of the software and the intellectual property that it may contain to the foundation -- this allows the foundation to obtain an irrevocable and permanent right to redistribute and work on the code, without fearing lock-in for itself or for its users.
- a sponsoring ASF member or officer -- this person will act as the main mentor, giving directions to the project, helping out in the day-to-day details and keeping contact with the incubator PMC.

The incubation period normally serves to estimate whether or not:

- the project is able to increase the diversity of its committer base and to play with the meritocratic rules of the foundation.

It might seem rather easy to achieve, but it must be remembered that in a volunteer and highly selective environment, attracting new committers is not automatic.

Diversity of committership is important for two main reasons:

- it gives long term stability to the project development: in fact, with all the developers affiliated to the same entity, the chance of seeing all of them moving away from the project at the same time is much greater than with a community of individuals affiliated to unrelated entities.
- it gives a greater variety of technical visions: something that guarantees a better adherence to environment and user's needs, thus a higher change of finding real-life use of the software.

Other Foundation Entities

Along with the Incubator, the foundation has several other cross-foundation projects. For example the ASF does not have offices or buildings, it's a virtual entity that exists only on the internet and the technical infrastructure that enables it to operate is managed by the Infrastructure team.

These and other cross-foundation projects are described on the Foundation Projects page.

The ASF also hosts some foundation-wide mailing lists, which are detailed on the Mailing Lists page.

In review...

Within the first 10 years of operation, the ASF represents one of the best examples of an open organization that has found balance between structure and flexibility. We have grown from 200 committers to around 3000, and that number continues to grow on a daily basis. We have been able to create several software products that are leaders in their market. We have also been able to find balance between openness and economical feasibility. This has earned us respect from a range of people, from single individuals to multinational corporations. We hope to continue to provide inspiration for businesses, governments, education, and for other software foundations.

Copyright © 2015 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

Free Software Support Network

“Free Projects, Free Communities”

Our Services

Accepting Tax-deductible Donations

FSSN is a recognized 501(c)(3) tax-exempt public charity. As a public charity FSSN can accept tax-deductible donations to support the goals of collaborating projects. Donors to FSSN may designate which collaborating projects the donation is intended to support. FSSN will then work with the collaborating project to use the donated funds in support of the project's mission. Whether a project receives a donation of a few dollars or tens of thousands of dollars, directing the funds to FSSN ensures responsible usage of funds for the benefit of the project and not any individual. It also avoids confusion about ownership of the funds.

The most common uses include paying for project members to travel to conferences, organizing conferences, paying for hosting fees, maintaining DNS registrations, purchasing of hardware, and registering and maintaining trademark registrations. All projects have unique needs and FSSN works closely with each project to ensure the funds are used to support the project's mission and only for furtherance of its charitable purpose.

Asset Management

FSSN can hold any assets on behalf of the Projects including DNS names, trademarks, copyrights, servers or testing hardware, or any other physical equipment. Projects often want continuity in the ownership of assets regardless of personnel changes within the project. While it is common for projects to initially register a DNS in a single person's name, managing the DNS registration over time can become an issue if that person stops actively contributing to a project. FSSN can hold assets on behalf of projects ensuring that the assets are used only for a charitable purpose and consistent with the project's goals.

Contracts Negotiation and Execution

FSSN can enter into contracts on behalf of the projects. Many projects work closely with commercial entities such as hardware or software companies. The personnel at FSSN have experience negotiating with commercial entities on behalf of FOSS developers. FSSN is experienced with negotiating agreements that protect not just individual developer's interests, but also the project's and the FOSS community's interests. FSSN can also enter into agreements on behalf of projects. This often eliminates the need for individual project members to negotiate individually with companies, and preventing the need to renegotiate agreements each time a new contributor joins a project.

Legal Assistance

Software Freedom Law Center provides free legal assistance and representation

to all of FSSN's collaborating projects. The attorneys at SFLC have experience representing the most well known FOSS projects (and not so well known projects). SFLC can provide collaborating projects with assistance in legal matters ranging from common questions on licensing compliance to complex negotiations with multinational corporations. Please see SFLC Services for further details.

Technical services

While most FOSS projects do not need technical assistance when it comes to running their own infrastructure, FSSN has experienced staff that can provide technical assistance when projects do not have the resources to do so themselves. Through special agreements with collaborating projects, FSSN can provide mailing list hosting, DNS hosting, or other common infrastructure services.

Fund Raising Assistance

FSSN collaborates with projects to raise funds for Project Activities and uses the funds in consultation with the Project for the furtherance of software freedom.

License Enforcement and Resolution

One of the most common reasons FOSS projects seek legal representation is to resolve violations of FOSS licenses.FSSN's relationship with the Software Freedom Law Center gives collaborating projects access to the most experienced attorney's in the area of FOSS community enforcement. SFLC defends the integrity of FOSS licenses against both adverse judicial interpretation and legislative

interference. SFLC also assists the general FOSS community in resolution of disputes relating to the use and development of FOSS. With the help of SFLC, FSSN strives to use licensing violations as opportunities to not just resolve the compliance issues, but also strengthen the collaborative FOSS ecosystem.

Officiating project elections

All FOSS projects are organized in a different manner, even if that organizational structure is unspoken. FSSN can act as a impartial third-party to help administer the election process to choose project leadership roles in accordance with the project's own rules. No matter the method from simple email balloting, on-line polls, first-past-the-post elections, or Condorcet voting systems, FSSN staff can act as a third party neutral in administering your election system.

© Free Software Support Network 2015

Software Freedom Conservancy

Members Projects & Services

Applying to Join Conservancy as a Member Project

Conservancy's Evaluation Committee considers applications monthly on a rolling basis. Currently, Conservancy has dozens of projects in various stages of the application process.

The application process is somewhat informal. New applicants should write an initial inquiry email to <apply@sfconservancy.org> with a very brief description of their project and a URL to their project's website. We'll send back initial questions (if any), and after those questions are answered, we'll send the full application materials. Applications should be submitted in plain ASCII text via email.

Projects are reviewed by Conservancy's Evaluation Committee, which is chartered by Conservancy's Board of Directors.

Project Membership Application FAQs

The following are various questions that we typically get from project leaders

that wish to apply to Conservancy.

I sent in my inquiry letter and/or application a long time ago. Why haven't you replied?

Conservancy receives an overwhelming level of interest and we have very few staff positions to meet the interest and demand for Conservancy's services to its member projects. Meanwhile, Conservancy always prioritizes needs of its existing member projects over new inquiries and applications. Therefore, it sometimes can take quite a while to finish the application process and be offered membership, but please note that such delays mean that should your project ultimately become a member project, your project will then be a beneficiary of this policy.

What are the key criteria our project must meet to join?

In order to join, projects need to meet certain criteria. A rough outline of those criteria are as follows:

- The project must be a software development or documentation project. Non-software projects to advance the cause of software freedom, while important and useful, are beyond the scope of Conservancy.
- The project must be exclusively devoted to the development and documentation of FLOSS. The project's goals must be consistent with Conservancy's tax-exempt purposes, and other requirements imposed on Conservancy by the IRS' 501(c)(3) rules. Namely, the goal of the project must to develop and document the software in a not-for-profit way to advance the public good, and must develop the software in public.
- The project must be licensed in a way fitting with software freedom principles. Specifically, all software of the project should be licensed under a license that is listed both as a Free Software license by the Free Software Foundation and as an Open Source license by the Open Source Initiative. All software documentation for the project should be licensed under a license on the preceding lists, or under Creative Commons' CC-By-SA or CC-By or CC-0.
- The project should have an existing, vibrant, diverse community that develops and documents the software. For example, projects that have been under development for less than a year or only a “proof of concept” implementation are generally not eligible.

While any project meeting the criteria above can apply, meeting these criteria doesn't guarantee acceptance of your project. Conservancy favors projects that are well-established and have some track record of substantial contributions from a community of volunteer developers. Furthermore, Conservancy does give

higher priority to projects that have an established userbase and interest, but also tries to accept some smaller projects with strong potential.

Is our project required to accept membership if offered?

Not at all. Many projects apply and subsequently decide not to join a non-profit, or decide to join a different non-profit entity. Don't worry about “wasting our time” if your project's developers aren't completely sure yet if they want to join Conservancy. If membership in Conservancy is currently a legitimate consideration for your project, we encourage you to apply. We'd rather that you apply and turn down an offer for membership than fail to apply and have to wait until the next application round when you're sure.

What benefits does our project get from joining?

We maintain a detailed list of services that Conservancy provides to member projects. If you have detailed questions about any of the benefits, please ask <apply@sfconservancy.org>.

Conservancy seems to be called a “fiscal sponsor” to its member projects. Does that mean you give our project money if we join?

It's true that we would love to fund our member projects if it were possible, because we believe they deserve to be funded. However, that's not typically what a fiscal sponsor does. The term “fiscal sponsor“ is often used in non-profit settings and has a standard meaning there. But, to those not familiar with non-profit operations, it comes across as a bit of a misnomer.

In this context, a fiscal sponsor is a non-profit organization that, rather than fund a project directly, provides the required infrastructure and facilitates the project's ability to raise its own funds. Conservancy therefore assists your project in raising funds, and allows your project to hold those funds and spend them on activities that simultaneously advance Conservancy's non-profit mission and the FLOSS development and documentation goals of the project.

What will the project leaders have to agree to if our project joins?

Once you're offered membership, Conservancy will send you a draft fiscal sponsorship agreement (FSA). A template of Conservancy's FSA is available in

PDF (and in ODT). Please note that the preceding documents are **only templates**. Please do not try to fill one out and send it to Conservancy. The final FSA between Conservancy and your project needs to be negotiated between us, and as can been seen in the template, the Representation section needs substantial work. If your project is offered membership, Conservancy will work with you adapt the FSA template to suit the needs and specific circumstances of your project. This is painstaking work, and it's better to complete that work after both Conservancy and the project are quite sure that they both want the project to join Conservancy.

If my project joins Conservancy, how will it change?

Substantively, member projects continue to operate in the same way as they did before joining Conservancy. So long as the project remains devoted to software freedom and operates consistently with the Conservancy's tax-exempt status, Conservancy does not intervene in the project's development other than to provide administrative assistance. For example, Conservancy keeps and maintains books and records for the project and assists with the logistics of receiving donations, but does not involve itself with technical or artistic decision making. Projects are asked, however, to keep Conservancy up to date on their activities.

Once our project joins, who holds its assets (money, copyrights, trademarks, etc.)?

Conservancy holds assets on behalf of its member projects and manages and disburses those assets in accordance with the wishes of the project's leadership. Funds received by Conservancy on behalf of a project are kept track of separately for each specific project and the management of those funds is directed by the project. For example, if a donor wanted to contribute $100 to Project Foo, they would formally make the donation to Conservancy and identify Project Foo as the desired project to support. Conservancy would then deposit the check and earmark the funds for use by Project Foo. Project Foo would then tell the Conservancy how that money should be spent. As long as that expense is a legitimate non-profit expense fitting with Conservancy's non-profit mission, Conservancy pays the expense on the Project's behalf.

Similarly, any copyrights, trademarks, domain name or other assets transferred to a project can also be held by Conservancy on behalf of the project. A significant service that Conservancy provides its members is a vehicle through which copyright ownership in the project can be unified. There are several advantages to having a consolidated copyright structure, including that it makes enforcement activity easier and more effective. However, copyright, trademark, and domain name assignment is not a requirement in order to join Conservancy,

rather, it is an option for those projects that ask for it.

If our project joins, must it be a member project of Conservancy forever?

All agreements between member projects and Conservancy stipulate clearly that the member project can leave Conservancy with a few months' notice. Federal tax exemption law, though, states that projects must transfer their assets from Conservancy in a way that is consistent with Conservancy's not-for-profit tax status — meaning the assets cannot be transferred to an individual or a for-profit entity. Generally, a project would either find another fiscal sponsor or form their own independent tax-exempt non-profit.

We fully expect that some Conservancy projects will ultimately wish to form their own non-profit 501(c)(3) organizations; that's why we design our agreements with projects to allow them to leave to another 501(c)(3) organization. Typically, projects join Conservancy because the project leaders don't want the burdens of running a non-profit themselves. Often, as projects grow, leaders get interested in the non-profit management and organizational side of the activities and are then prepared to take on the additional work themselves.

How are “project leaders” defined with respect to Conservancy?

How leaders are chosen for projects varies greatly from project to project. Our goal is to do our best to embody the “natural” leadership structure that evolved in your project into the formal agreement with Conservancy. As part of the agreement drafting, we work carefully with you to understand your project's governance and write up formally with you the decision-making process you use. Most project contributors find this process of formalizing the leadership structure helps them clarify in their own minds the governance of their project, even though the process can be difficult. Since it can be a complicated process, we suggest that you prepare your project community for this discussion once your project is accepted.

How much does it cost us financially to join Conservancy?

New Conservancy members are required to pay 10% of their revenue that Conservancy processes to Conservancy's general fund, which primarily is used to pay staff. (Details on how Conservancy spends its funds, including salaries of key employees, can be found in Conservancy's annual filings.)

Historically, Conservancy allowed projects to give less or nothing at all to the general fund, but we unfortunately discovered that without this requirement, Conservancy was not able to offer the myriad of services to all its projects, particularly to larger projects that have more income and therefore need more attention from staff.

We do understand that, particularly for small projects that only receive a few small donations, that donating a percentage of your income back to Conservancy can be a high burden. Therefore, Conservancy remains open to discussion on a case-by-case basis for smaller projects about how to handle this requirement, and applicants should feel free to raise any concerns about this issue during the application process.

Follow Conservancy on identi.ca and twitter. Flattr this!

This page, and all contents herein, unless a license is otherwise specified, are licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Software Freedom Conservancy

Members Projects & Services

Member Project Services

Conservancy assists FLOSS project leaders by handling all matters other than software development and documentation, so the developers can focus on what they do best: improving the software for the public good. The following are the services and options that are available to FLOSS projects that have joined Conservancy as a member project.

Tax-Deductible, Earmarked Donations

Member projects can receive earmarked donations through Conservancy. Since Conservancy is a 501(c)(3) charity incorporated in New York, donors can often deduct the donation on their USA taxes. Additionally, the donors can indicate that their donation should be used to advance a specific member project, and those funds are kept in a separate account for the member project by Conservancy. This structure prevents developers from having to commingle project funds with their own personal accounts or having to set up their own project specific account.

Since Conservancy is a tax-exempt organization, there are some limits that the law places on what member projects can do with their assets, but those limits are the same as if the project was an independent non-profit entity. Usually, the project leadership instructs Conservancy's leadership on how the project's funds are spent. Conservancy spends these funds on the project's behalf on any

expenses that constitute appropriate activity under Conservancy's 501(c)(3) not-for-profit mission. Some typical uses of earmarked donations by Conservancy's member projects are:

- funding travel expenses for project developers to attend relevant conferences.
- domain name fees, bandwidth costs, and computer equipment purchases.
- purchasing media for distribution of project software at conferences and events.
- paying key developers on a contractual basis to improve the project's software and its documentation.
- sponsoring and organizing conferences for the project.
- trademark registration and enforcement.
- FLOSS license enforcement and compliance activity.

Asset Stewardship

Conservancy can hold any assets for the project on its behalf. This includes copyrights, trademarks, domain names, physical computer equipment or anything that should be officially held in the name of the project. Member projects are not required that Conservancy hold all assets of a project. (For example, member projects are not *required* to assign copyrights to Conservancy.) However, Conservancy can accommodate the needs of projects that want their assets under the control of a not-for-profit entity and exercised only for the public good.

Contract Negotiation and Execution

Projects sometimes need to negotiate and execute a contract with a company. For example, when a project wants to organize and run a conference, the venue usually has a complicated contract for rental of the space and services. Conservancy assists projects in the negotiation of such contracts, and can sign them on behalf of the project.

Conference Logistical Support

Many Conservancy projects have an annual conference. Conservancy provides logistical support for these conferences, particularly in the area of financial responsibility and liability. Conservancy provides a small amount of logistical support for conference in other ways, resource-permitting.

Basic Legal Advice and Services

Since projects, upon joining, become organizationally part of Conservancy,

Conservancy can provide basic legal services to its member projects through Conservancy's own General Counsel, outside counsel, and pro-bono attorneys. For example, Conservancy assists its projects in handling issues related to trademark registration, trademark policy development and licensing, trademark enforcement, copyright licensing and enforcement, and non-profit governance questions and issues.

FLOSS Copyright License Enforcement

Complying with FLOSS licenses is easy, as they permit and encourage both non-commercial and commercial distribution and improvements. Nevertheless, violations of FLOSS licenses (in particular of the GPL and LGPL) are all too common. At request of the project's leaders, Conservancy can carry out license enforcement activity on behalf of the project's copyright holders.

Fundraising Assistance

Conservancy provides various tools and advice to member projects on methods of raising funds for their projects' earmarked accounts.

Avoid Non-Profit Administrivia

Member projects can continue to operate in the same way they did before joining Conservancy without having to select a board of directors or any other layer of corporate management, without having to maintain corporate records and without having to do any of the other things required of incorporated entities. Conservancy handles all of that burden on behalf of its projects.

Leadership Mentoring, Advice and Guidance

Many of Conservancy's directors are experienced FLOSS project leaders. They offer themselves as a resource to member project leaders who need assistance or face challenges in their work leading their projects.

Some Personal Liability Protection

When a project joins Conservancy, it formally becomes part of the Conservancy. (The project is thus somewhat analogous to a division of a company or a department in a large agency.) As such, project leaders benefit from some amount of protection from personal liability for their work on the project.

Officiating Community Elections and Ballot

Initiatives

Conservancy will organize and run community leadership committee elections and/or ballot initiatives for its member project communities, using online voting software.

Those familiar with non-profit terminology will recognize most of these services as fiscal sponsorship services. This term is not particularly well known in the FLOSS community, and many are confused by that term. However, if you are familiar with what a fiscal sponsor typically does in the non-profit sector, the term does fit many of services that Conservancy offers its member projects.

Project leaders that believe their project might benefit from these services can apply to become a member project.

Follow Conservancy on identi.ca and twitter. Flattr this!

This page, and all contents herein, unless a license is otherwise specified, are licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Associated Project HowTo

Link from: http://spi-inc.org/projects/associated-project-howto/

Free and open source projects that are deemed to be genuine, substantial and significant may be eligible for associated project status.

Projects interested in becoming SPI associated projects should review these documents:

- Relationship between SPI and an associated project
- Services offered to an associated project

There is no cost to become or remain an associated project.

The Application Process

Informal Discussions

Generally the process starts with informal discussions between project representatives and one or more board members, initiated either by the project representatives or the board members. These discussions carry no committment on either side and are an opportunity for the project and SPI to establish if proceeding to a formal application makes sense for the project.

Projects interested in becoming SPI associated projects are welcome to contact the board for a discreet informal discussion on whether the project is likely to be accepted as an associated project. As this stage the board may offer advice that will improve the chance of acceptance later.

If a board member is personally satisfied that the project is suitable for associated project status they may agree to sponsor the project's application.

Formal Application

If the project wishes to proceed, a formal application is sent to the sponsor.

The information needed is:

1. The name and details of the project
2. Which SPI services will be needed
3. Who is going to be the liaison to SPI, and the process for selecting/electing replacements

Note: (2) above does not exclude the use of additional SPI services. This information is sought so that SPI can assess short term service requirements.

Following the formal application, and any additional discussion, the sponsor will draft a resolution

similar to the template below if they are still satisfied that the project is suitable for associated project status.

```
SPI resolution YYYY-MM-DD.xyz.1

WHEREAS

1. [Project] is a substantial and significant Free Software project.

2. The [Project] developers would like SPI's support and assistance, including
   taking donations.

THE SPI BOARD RESOLVES THAT

3. [Project] is formally invited to become an SPI Associated Project, according
   to the SPI Framework for Associated Projects, SPI Resolution
   1998-11-16.iwj.1-amended-2004-08-10.iwj.1, a copy of which can be found at
   http://www.spi-inc.org/corporate/resolutions/2004/2004-08-10.iwj.1/

4. [Liaison] is recognised by SPI as the authoritative decision maker
   and SPI liaison for [project].  Successors will be appointed
   [describe method of selection or election].

5. This invitation will lapse, if not accepted, 60 days after it is approved by
   the SPI Board.
```

Discussion

This resolution will be presented to the board and contributing members, and discussed. If the project is in some way political or controversial, it may be necessary to champion it to the SPI contributing membership. This process is not intended to be adversarial - the members just want to avoid any difficult-to-rectify mistakes.

After at least three days of discussion, the resolution may be submitted for a vote at an SPI board meeting, which are held monthly on irc.spi-inc.org (the OFTC network), channel #spi, according to a schedule published on the SPI web site. These meetings are public and all are welcome to attend.

Vote

Board members will judge the application on several merits:

Free Software: is the project a genuine Free Software community project?

Substance: Does the project have an established development community, history of software releases, etc?

Significance: Is the project used by a broad audience, or does it have political or market significance?

Acceptance

If the resolution passes, the project is invited to become an associated project. The nominated liaison

will be notified of the invitation. They will then have the amount of time stated in the resolution, usually 60 days, to officially accept.

The Project Liaison

The Liaison is the person from the project to whom the Board listens for all authoritative decisions regarding project assets, fundraising, expenses and disposition. While the Board is happy to talk to other members of the project, only the Liaison will be able to send any instructions regarding funds or assets, unless they delegate someone else.

The SPI Board does not stipulate how the Liaison is chosen in the project, as long as there are clear rules which let the Board know to whom to listen, especially in the event of disagreement. For most projects, it is simply one of the project founders who volunteers and appoints their own successor. A few projects, such as Debian and PostgreSQL, have well defined election procedures.

It is recommended, but not required, that the Liaison attend Board meetings. At Board meetings, Liaisons are considered "Advisors", able to bring proposals to the Board and speak but not to vote (unless, of course, they also happen to be Board members).

Participating in SPI

Contributors to the project are eligible for SPI contributing membership subject to the guidelines set out here but they each have to apply for it individually. The liaison can speed up the membership acceptance process by supplying the Board and Membership Committee with a list of eligible contributors for the project. The liaison will be consulted where there is doubt.

As the Contributing members elect the Board, as well as argue decisions which the Board feels are controversial enough to merit wide discussion, it is important that the project members join SPI to ensure the project is well represented.

Fundraising

All monetary activities in SPI are administrated by the Treasurer (treasurer@spi-inc.org).

SPI can accept donations for the project in two ways: checks or credit cards. Checks must be in American or Canadian dollars and are mailed directly to SPI's mailing address. Credit cards are processed by an external service, Click&Pledge at this time. The Treasurer should be contacted to set up access to credit card donations, which may include the ability to create special donation pages for individual campaigns or events for which the project is collecting.

In either case, it is important that the donor designate that the gift is to go to the project. If a gift arrives without a designated project, the Treasurer will attempt to contact the donor, and if unsuccessful will place the money in the SPI general fund.

Please note that as a US 501(c)3 Non-Profit Organization, there are legal restrictions on what money SPI can accept. Most common project fundraising activities are fine, but if the project plans to do anything unusual, please clear it with the treasurer first. Sales of fixed-price items (like T-shirts) are acceptable but the Treasurer needs to know about how the money was collected.

All donations to SPI are charitable under US law, except in certain cases such as t-shirt sales and event tickets. As a US non-profit, SPI is unable to provide donation tax credits to residents of other countries.

All transaction costs (such as the 4.5% for credit cards, and wire transfer fees) are deducted from the contribution. 5% of the remainder is deducted for SPI overhead, primarily accounting, photocopying and postage. The remaining money is held in trust for the project.

Due to processing time, it can take between a few days and a few weeks for a donation to arrive in the bank account and be available to the project. Under unusual circumstances an associated project can draw money from the SPI reserves against donations which are confirmed (i.e. check received) but not deposited, but this is not normal practice.

The liaison will receive notice of any donations made to the project, with donor details if available. It is recommended to send personalized thank-you e-mails or letters to project donors.

Paying Project Expenses

The liaison can request payment of project expenses at any time by sending a request to the treasurer. If the expense is legal, it will be paid as soon as the Treasurer can reasonably manage it. Please note that paying expenses usually means mailing checks, so payment generally takes two weeks or more.

Requests for payment should be accompanied by paperwork detailing the expense. If the paperwork is not electronic, it can be faxed or posted. Generally, it is expected that individuals will pay the expenses up front and be reimbursed by SPI, but advance payment can be arranged with sufficient advance warning to the treasurer. The Treasurer also has a credit card for online purchases which for some reason need to be made directly by SPI.

There are tax law restrictions on what SPI can legally pay for as a 501(c)3 Non-Profit. Common expenses like travel, equipment, flyers, booths, conference expenses and legal help are generally fine, but some items like software development contracting need to be handled carefully. If the liaison is in doubt they should contact the Treasurer.

Transaction fees from paying expenses (wire transfer fees, cashier's checks and postage) will be paid out of project funds. Funds may be transferred only to other 501(c)3 US non-profit organizations, and may not be transferred to private companies, other types of non-profits, or foreign organizations except in compensation.

The Treasurer will give the liaison a monthly report of donations collected and expenses paid for the project.

Copyright © 2010-2011 Software in the Public Interest, Inc.
License: Creative Commons Attribution-ShareAlike 3.0 Unported

Relationship Between SPI and Associated Projects

Link from: http://spi-inc.org/projects/relationship/

Fiscal Sponsorship

SPI acts as a fiscal sponsor for associated projects.

Project Independence

SPI does not own, govern or control the associated projects. All actions by SPI on behalf of associated projects must comply with relevant laws, SPI's By-Laws and 501(c)3 status. SPI does not prohibit the project having a similar relationship with other fiscal sponsors.

Freedom to Leave

The project liaison may decide that the project is leaving SPI at any time. Any assets and money held by SPI for the project may be transferred to a 501(c)3 US non-profit of the liaison's choice, or simply held until expended.

Liability

SPI does not indemnify associated projects or members.

Copyright © 2010-2011 Software in the Public Interest, Inc.
License: Creative Commons Attribution-ShareAlike 3.0 Unported

Services Offered to Associated Projects

Link from: http://spi-inc.org/projects/services/

SPI offers a variety of services to associated projects. The major services offered by SPI are listed here. Additional services may be offered at the discretion of the board.

If a project wishes to use one of these services the project liaison should contact the board which will make arrangements as appropriate.

Accepting Donations and Holding Funds

SPI will accept donations and hold funds on behalf of associated projects. Refunds for legitimate project expenses will be made from funds earmarked for an associated project with the consent of the project liaison. Donations to associated projects by US residents are normally tax deductible. SPI does not assist with fundraising activities.

Once held by SPI, funds may only be transferred to another 501(c)3 US non-profit.

Holding Substantial Assets

Substantial equipment, software or other assets valued at over $300 which an associated project purchases with SPI funds are owned by SPI.
SPI will also accept donations of assets on behalf of associated projects. The equipment will be used and maintained by the project but SPI will hold legal ownership.

Once held by SPI, substantial assets may only be transferred to another 501(c)3 US non-profit.

Holding Intangible Assets

Associated projects may transfer intangible assets such as domain names, trademarks and licenses to SPI for protection. In addition SPI can seeking to obtain trademarks on behalf of associated projects.

Once held by SPI, intangible assets may only be transferred to another 501(c)3 US non-profit.

Signing Contracts

SPI can sign contracts on behalf of associated projects.

Examples include:

- Signing a contract with a venue for an associated project to hold a conference
- Signing a contract for insurance for events held by an associated project

Any costs associated with the contract are borne out of SPI funds earmarked for that associated project.

Legal Assistance

SPI has access to legal counsel which the board may consult on behalf of the project, at the discretion of the board.

Technical Services

SPI can provide technical services (such as the provision of authoritative nameservers) for a project, at the discretion of the board.

Copyright © 2010-2011 Software in the Public Interest, Inc.
License: Creative Commons Attribution-ShareAlike 3.0 Unported

News Essentials

- What's Hot
- News Releases
- IRS - The Basics
- IRS Guidance
- Media Contacts
- Facts & Figures
- Around the Nation
- e-News Subscriptions

The Newsroom Topics

- Multimedia Center
- Noticias en Español
- Radio PSAs
- Tax Scams
- The Tax Gap
- Fact Sheets
- IRS Tax Tips
- Armed Forces
- **Latest News Home**

New 1023-EZ Form Makes Applying for 501(c)(3) Tax-Exempt Status Easier; Most Charities Qualify

IRS YouTube Video
Form 1023-EZ: English | Spanish | ASL

IR-2014-77, July 1, 2014

WASHINGTON — The Internal Revenue Service today introduced a new, shorter application form to help small charities apply for 501(c)(3) tax-exempt status more easily.

“This is a common-sense approach that will help reduce lengthy processing delays for small tax-exempt groups and ultimately larger organizations as well,” said IRS Commissioner John Koskinen. “The change cuts paperwork for these charitable groups and speeds application processing so they can focus on their important work."

The new Form 1023-EZ, available today on IRS.gov, is three pages long, compared with the standard 26-page Form 1023. Most small organizations, including as many as 70 percent of all applicants, qualify to use the new streamlined form. Most organizations with gross receipts of $50,000 or less and assets of $250,000 or less are eligible.

"Previously, all of these groups went through the same lengthy application process -- regardless of size," Koskinen said. "It didn't matter if you were a small soccer or gardening club or a major research organization. This process created needlessly long delays for groups, which didn’t help the groups, the taxpaying public or the IRS.”

The change will allow the IRS to speed the approval process for smaller groups and free up resources to review applications from larger, more complex organizations while reducing the application backlog. Currently, the IRS has more than 60,000 501(c)(3) applications in its backlog, with many of them pending for nine months.

Following feedback this spring from the tax community and those working with charitable groups, the IRS refined the 1023-EZ proposal for today's announcement, including revising the $50,000 gross receipts threshold down from an earlier figure of $200,000.

"We believe that many small organizations will be able to complete this form without creating major compliance risks," Koskinen said. "Rather than using large amounts of IRS resources up front reviewing complex applications during a lengthy process, we believe the streamlined form will allow us to devote more compliance activity on the back end to ensure groups are actually doing the charitable work they apply to do."

The new EZ form must be filed online. The instructions include an eligibility checklist that organizations must complete before filing the form.

The Form 1023-EZ must be filed using pay.gov, and a $400 user fee is due at the time the form is submitted. Further details on the new Form 1023-EZ application process can be found in Revenue Procedure 2014-40, posted today on IRS.gov.

There are more than a million 501(c)(3) organizations recognized by the IRS.

Related Item: Information on Form 1023-EZ

Follow the IRS on New Media
Subscribe to IRS Newswire

Page Last Reviewed or Updated: 18-Jun-2015

Instructions for Form 1023-EZ

(Rev. August 2015)

Streamlined Application for Recognition of Exemption Under Section 501(c)(3) of the Internal Revenue Code

Department of the Treasury
Internal Revenue Service

Section references are to the Internal Revenue Code unless otherwise noted.

Contents **Page**

General Instructions 1
- Purpose of Form 1
- Who Can File This Form 1
- How To File 1
- User Fee 2
- When To File (Effective Date of Exemption) 2
- Filing Assistance 2
- Signature Requirements 2
- Annual Filing Requirements 2
- Public Inspection 2
- State Registration Requirements 2

Specific Instructions 3
- Part I. Identification of Applicant 3
- Part II. Organizational Structure 3
- Part III. Your Specific Activities 5
- Part IV. Foundation Classification 8
- Part V. Reinstatement After Automatic Revocation 10
- Part VI. Signature 10

Form 1023-EZ Eligibility Worksheet (Must be completed prior to completing Form 1023-EZ) 11

National Taxonomy of Exempt Entities (NTEE) Codes. 18

Future Developments

For the latest information about developments related to Form 1023-EZ and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/form1023*.

Reminder

Do not include social security numbers on publicly disclosed forms. Because the IRS is required to disclose approved exemption applications and information returns, exempt organizations should not include social security numbers on these forms. Documents subject to disclosure include correspondence with the IRS about the filing.

Photographs of Missing Children

The Internal Revenue Service is a proud partner with the National Center for Missing and Exploited Children. Photographs of missing children selected by the Center may appear in instructions on pages that would otherwise be blank.You can help bring these children home by looking at the photographs and calling 1-800-THE-LOST (1-800-843-5678) if you recognize a child.

Email Subscription

The IRS has established a subscription-based email service for tax professionals and representatives of tax-exempt organizations. Subscribers will receive periodic updates from the IRS regarding exempt organization tax law and regulations, available services, and other information. To subscribe, visit *www.irs.gov/charities*.

General Instructions

"You" and "Us". Throughout these instructions and Form 1023-EZ, the terms "you" and "your" refer to the organization that is applying for tax-exempt status. The terms "us" and "we" refer to the Internal Revenue Service.

Purpose of Form

Form 1023-EZ is the streamlined version of Form 1023, Application for Recognition of Exemption Under Section 501(c)(3) of the Internal Revenue Code. Any organization may file Form 1023 to apply for recognition of exemption from federal income tax under section 501(c)(3). Only certain organizations are eligible to file Form 1023-EZ (see *Who Can File This Form* below).

Note. Most organizations seeking exemption from federal income tax under section 501(c)(3) are required to complete and submit an application. However, the following types of organizations may be considered tax exempt under section 501(c)(3) even if they do not file Form 1023 or Form 1023-EZ.

- Churches, including synagogues, temples, and mosques.
- Integrated auxiliaries of churches and conventions or associations of churches.
- Any organization that has gross receipts in each taxable year of normally not more than $5,000.

Who Can File This Form

Only certain organizations are eligible to apply for exemption under section 501(c)(3) using Form 1023-EZ. To determine if you are eligible to file Form 1023-EZ, you must complete the Form 1023-EZ Eligibility Worksheet.

CAUTION *If you answer "Yes" to **any** of the worksheet questions, you are not eligible to apply for exemption under section 501(c)(3) using Form 1023-EZ. You must apply on Form 1023. If you answer "No" to **all** of the worksheet questions, you may apply using Form 1023-EZ.*

TIP *Before completing either Form 1023 or Form 1023-EZ, we recommend reading "Life Cycle of an Exempt Organization" at www.irs.gov/charities.*

How To File

The Form 1023-EZ can only be filed electronically by going to *www.irs.gov/form1023* or *www.pay.gov* (enter the term "Form 1023-EZ" in the search box). We will not accept printed copy submissions of the application.

We recommend you preview and print a copy of your application for your records before submitting it electronically.

User Fee

A user fee of $400 is required to process your application. This fee must be paid through *www.pay.gov* when you file your application. Payments can be made directly from your bank account or by credit/debit card.

When To File (Effective Date of Exemption)

Generally, if you file Form 1023-EZ within 27 months after the end of the month in which you were legally formed, and we approve the application, the legal date of formation will be the effective date of your exempt status.

If you do not file Form 1023-EZ within 27 months of formation, the effective date of your exempt status will be the date you filed Form 1023-EZ (submission date).

If you do not file Form 1023-EZ within 27 months of formation, and you believe you qualify for an earlier effective date than the submission date, you can request the earlier date by sending correspondence to the address below. The correspondence should include your name, employer identification number (EIN), the effective date you are requesting, an explanation of why the earlier date is warranted, and any supporting documents. This correspondence should be sent after you receive your Determination Letter. Alternatively, you may complete Form 1023 in its entirety instead of completing Form 1023-EZ.

Note. If you have been automatically revoked and are seeking retroactive reinstatement, see Part V. Reinstatement After Automatic Revocation of these instructions.

Send effective date correspondence to:

Internal Revenue Service
Exempt Organizations Determinations
Room 4024
P.O. Box 2508
Cincinnati, OH 45201

Application process

Submitting this application does not guarantee exemption will be recognized. If your application is incomplete or not completed correctly, it may be rejected. In addition, you may be contacted for additional information. Also, the IRS will select a statistically valid random sample of applications for pre-determination reviews, which may also result in requests for additional information.

Filing Assistance

For help in completing this form or general questions relating to an exempt organization, call Exempt Organization Customer Account Services toll free at 1-877-829-5500. You may also access information on our website at *www.irs.gov/charities*.

The following publications are available to you for further information.

- *Publication 517, Social Security and Other Information for Members of the Clergy and Religious Workers*
- *Publication 526, Charitable Contributions*
- *Publication 557, Tax-Exempt Status for Your Organization*
- *Publication 598, Tax on Unrelated Business Income of Exempt Organizations*
- *Publication 1771, Charitable Contributions–Substantiation and Disclosure Requirements*
- *Publication 1828, Tax Guide for Churches and Religious Organizations*
- *Publication 3079, Tax-Exempt Organizations and Gaming*
- *Publication 3833, Disaster Relief: Providing Assistance Through Charitable Organizations*
- *Publication 4220, Applying for 501(c)(3) Tax-Exempt Status*
- *Publication 4221, Compliance Guide for 501(c)(3) Tax-Exempt Organizations*

Signature Requirements

An officer, director, or trustee listed in Part I, line 8, who is authorized to sign for the organization must sign Form 1023-EZ. The signature must be accompanied by the title or authority of the signer and the date.

Annual Filing Requirements

Generally, an organization that qualifies for exemption under section 501(c)(3) is required to file an annual return in accordance with section 6033(a). However, an eligible organization, other than a private foundation, that normally has gross receipts of less than $50,000 is not required to file an annual return, but must furnish notice on Form 990-N (e-Postcard) providing the information required by section 6033(i). See Rev. Proc. 2011-15, 2011-3 I.R.B. 322.

An organization that is required to file a Form 990-series annual information return or submit an annual electronic notice, Form 990-N, must do so even if its application for recognition of exemption has not been filed or has been filed but not yet approved.

If an annual information return or tax return is due while the Form 1023-EZ is pending, complete the return, check the "Application pending" box in the heading, and send the return to the address indicated in the instructions.

If an annual electronic notice, Form 990-N, is due while the Form 1023-EZ is pending, the organization may need to contact the IRS at 1-877-829-5500 and ask for an account to be established for the organization so that it may file the notice.

Information on annual information return and electronic notice filing requirements and exceptions to the filing requirements may be found in Publication 557 and at *www.irs.gov/charities*.

If you believe you meet an exception to filing Form 990, Return of Organization Exempt From Income Tax; Form 990-EZ, Short Form Return of Organization Exempt From Income Tax; or Form 990-N, then you may request IRS recognition of this exception by filing Form 8940, Request for Miscellaneous Determination. A user fee must accompany the form. Alternatively, you may complete Form 1023 in its entirety instead of completing Form 1023-EZ.

Note. You do not need to notify the IRS that you are excepted from the annual filing requirement under section 6033(a) if your basis for the exception is that you are not a private foundation, your gross receipts are normally less than $50,000, and you are filing Form 990-N.

Public Inspection

Information available for public inspection. If we approve exempt status under section 501(c)(3), both you and the IRS must make your application and related documents available for public inspection. For more information, please go to *www.irs.gov/Charities-&-Non-Profits/Exempt-Organization-Public-Disclosure-and-Availability-Requirements*.

State Registration Requirements

Tax exemption under section 501(c)(3) is a matter of federal law. After receiving federal tax exemption, you may also be required

to register with one or more states to solicit contributions or to obtain exemption from state taxes. The National Association of State Charity Officials (NASCO) maintains a website that provides informational links to the various states for these purposes. It can be accessed at *www.nasconet.org*.

Donor Reliance on a Favorable Determination

Generally, donors and contributors may rely on an organization's favorable Determination Letter under section 501(c)(3) until the IRS publishes notice of a change in status, unless the donor or contributor was responsible for or aware of the act or failure to act that results in the revocation of the organization's Determination Letter. See Rev. Proc. 2011-33, 2011-25 I.R.B. 887.

Specific Instructions

Before completing the Form 1023-EZ, you must complete the Form 1023-EZ Eligibility Worksheet. If you meet the eligibility requirements, you must check the box at the top of Form 1023-EZ to attest that you are eligible to file the form. By checking the box, you are also attesting that you have read and understand the requirements to be exempt under section 501(c)(3). You are not required to submit the eligibility worksheet with your form. However, you should retain the worksheet for your records.

Part I. Identification of Applicant

Line 1a. Full name of organization. Enter your complete name exactly as it appears in your organizing document, including amendments.

Line 1b – 1e. Mailing address. Enter your complete address where all correspondence will be sent. If mail is not delivered to the street address and you have a P.O. box, enter your box number instead of the street address.

Line 2. Employer identification number (EIN). Enter the nine-digit EIN assigned to you.

You will not be able to submit this application until you have obtained an EIN.

An EIN is required regardless of whether you have employees. If you need an EIN, you may apply online at *www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Apply-for-an-Employer-Identification-Number-(EIN)-Online*, or you can apply for one by:

1. Mailing Form SS-4 to the IRS at the address provided in the Instructions for Form SS-4.
2. Faxing Form SS-4 to the fax number provided in the Instructions for Form SS-4.

You can access Form SS-4 online at *www.irs.gov*, or to order IRS tax forms and publications go to *www.irs.gov/orderforms*. If you previously applied for an EIN and have not yet received it, or you are unsure whether you have an EIN, please call our toll-free customer account services number, 1-877-829-5500, for assistance.

Line 3. Month tax year ends (01-12). Enter the month that your tax year (annual accounting period) ends, using a two-digit number format. For example, if your annual accounting period ends December 31, enter "12." Your annual accounting period is the 12-month period on which your annual financial records are based. Your first tax year could be less than 12 months. Check your bylaws or other rules of operation for consistency with the annual accounting period entered on line 3.

Line 4. Person to contact if more information is needed. Enter the name and title of the person to contact if more information is needed. The person to contact may be an officer, director, trustee, or other individual who is permitted to speak with us according to your bylaws or other rules of operation. Your person to contact may also be an "authorized representative," such as an attorney, certified public accountant (CPA), or enrolled agent (EA).

Note. We will request a Form 2848, Power of Attorney and Declaration of Representative, if we need to contact an authorized representative for additional information.

Line 5. Contact telephone number. Provide a daytime telephone number for the contact listed on line 4.

Line 6. Fax number. Provide a fax number for the contact listed on line 4.

Line 7. User fee submitted. Enter the user fee amount paid. (The current user fee is $400.)

Line 8. List the names, titles, and mailing addresses of your officers, directors, and/or trustees. Enter the full names, titles, and mailing addresses of your officers, directors, and/or trustees. You may use the organization's address for mailing. If you have more than five, list only five in the order below.

1. President or chief executive officer or chief operating officer.
2. Treasurer or chief financial officer.
3. Chairperson of the governing body.
4. Any officers, directors, and trustees who are substantial contributors (not already listed above).
5. Any other officers, directors, and trustees who are related to a substantial contributor (not already listed above).
6. Voting members of the governing body (not already listed above).
7. Officers (not already listed above).

If an individual serves in more than one office (for example, as both an officer and director), list this individual on only one line and list all offices held.

An officer is a person elected or appointed to manage the organization's daily operations, such as president, vice president, secretary, treasurer, and, in some cases, board chair. The officers of an organization are determined by reference to its organizing document, bylaws, or resolutions of its governing body, or otherwise designated consistent with state law.

A director or trustee is a member of the organization's governing body, but only if the member has voting rights.

Line 9a. Organization's website. Enter your current website address, as of the date of filing this application. If you do not maintain a website, enter "N/A" (not applicable).

Line 9b. Organization's email. Enter your email address to receive educational information from us in the future. Because of security concerns, we cannot send confidential information via email.

Part II. Organizational Structure

Line 1. Entity type. Only certain corporations, unincorporated associations, and trusts are eligible for tax-exempt status under section 501(c)(3) of the Code. Sole proprietorships, partnerships, and loosely affiliated groups of individuals are not eligible. Check the appropriate box to indicate whether you are a corporation, an association, or a trust.

Note. Even though certain limited liability companies (LLCs) are eligible to receive exemption under section 501(c)(3), they are not eligible to apply for exemption using this form.

Corporation. A "corporation" is an entity organized under a federal or state statute, or a statute of a federally recognized Indian tribal or Alaskan native government. A corporation's organizing document is generally referred to as its "articles of incorporation." A corporation must be incorporated under the non-profit or non-stock laws of the jurisdiction in which it incorporates.

Unincorporated association. An "unincorporated association" formed under state law must have at least two members who have signed a written document for a specifically defined purpose.

Trust. A trust may be formed by a trust agreement or a declaration of trust. A trust may also be formed through a will.

Line 2. Necessary organizing document. See below for your organization type.

Corporation. If incorporated under a federal, state, or federally recognized Indian tribal or Alaskan native government statute, you have a "necessary organizing document" if your organizing document shows certification of filing. This means your organizing document shows evidence that on a specific date it was filed with and approved by an appropriate state authority.

Unincorporated association. In order to be a "necessary organizing document," your articles of organization must include your name, your purpose(s), the date the document was adopted, and the signatures of at least two individuals.

Bylaws may be considered an organizing document only if they are properly structured to include your name, purpose(s), signatures, and intent to form an organization.

Trust. In order for your trust agreement or declaration of trust to be a "necessary organizing document," it must contain appropriate signature(s) and show the exact date it was formed.

Line 3. Formation date. See below for your organization type.

Corporation. If you are a corporation, you should enter the date that the appropriate authority filed your articles of incorporation or other organizing document.

Unincorporated association. If you are an unincorporated association, you should enter the date that your organizing document was adopted by the signatures of at least two individuals.

Trust. If your trust was formed by a trust agreement or a declaration of trust and does not provide for distributions to non-charitable interests, enter the date the trust was funded. Generally, a trust must be funded with property, such as money, real estate, or personal property, to be legally created.

If your trust document provides for distributions for non-charitable interests, enter the date on which these interests expired. If your trust agreement continues to provide for non-charitable interests, you will not qualify for tax-exempt status.

If you were formed by a will, enter the date of death of the testator or the date any non-charitable interests expired, whichever is later.

Note. If you amended your organizational documents to comply with the requirements of section 501(c)(3), enter the date of amendment, unless the amendment was nonsubstantive within the meaning of Rev. Proc. 2015-5.

Line 4. State of formation. Enter the jurisdiction (for instance, the state or the federally recognized tribal government) under the laws of which you were incorporated or otherwise formed. If you are a corporation, this may not be the place in which you are physically located. For example, if you are physically located in New York, but incorporated under Massachusetts law, enter Massachusetts.

Line 5. Purpose(s) clause. Your organizing document must limit your purposes to those described in section 501(c)(3). Those purposes are: charitable, religious, educational, scientific, literary, testing for public safety, fostering national or international amateur sports competition, and preventing cruelty to children or animals. See discussion of these purposes under Part III, line 2 of these instructions.

If your purposes are limited by referring to section 501(c)(3), your organizing document also properly limits your purposes. For example, the phrase "relief of the elderly within the meaning of section 501(c)(3)" in your organizing document also properly limits your purposes.

However, if the purposes listed in your organizing document are broader than those listed in section 501(c)(3), you should amend your organizing document before applying for recognition of exemption. A reference to section 501(c)(3) will not ensure that your purposes are limited to those described in section 501(c)(3). All of the language in your organizing document must be considered. The following is an example of an acceptable purpose clause:

The organization is organized exclusively for charitable, religious, educational, and scientific purposes under section 501(c)(3) of the Internal Revenue Code, or corresponding section of any future federal tax code.

See Publication 557 for further information and examples of how to limit your purposes.

Line 6. Activities not in furtherance of exempt purposes. Your organizing document must not expressly empower you to engage, otherwise than as an insubstantial part of your activities, in activities that in themselves are not in furtherance of one or more exempt purposes described in section 501(c)(3). In other words, you are not organized exclusively for one or more exempt purposes if your organizing documents expressly empower you to carry on activities that further purposes outside the scope of section 501(c)(3), such as "to engage in the operation of a social club" or "to engage in a manufacturing business," regardless of the fact that your organizing document may state that you are created for "charitable purposes within the meaning of section 501(c)(3) of the Code."

Further, your net earnings must not inure to the benefit of private shareholders or individuals. You must establish that you will not be organized or operated for the benefit of private interests, such as the creator or the creator's family, shareholders of the organization, other designated individuals, or persons controlled directly or indirectly by such private interests. Also, you must not, as a substantial part of your activities, attempt to influence legislation (however, eligible organizations may elect an expenditure limit instead of the "no substantial part" limit), and you are prohibited from participating to any extent in a political campaign for or against any candidate for public office.

The following is an example of an acceptable clause:

No part of the net earnings of the corporation shall inure to the benefit of, or be distributable to its members, trustees, officers, or other private persons, except that the corporation shall be authorized and empowered to pay reasonable compensation for services rendered and to make payments and distributions in furtherance of the purposes described in section 501(c)(3). No substantial part of the activities of the corporation shall be the carrying on of propaganda, or otherwise attempting to influence legislation, and the corporation shall not participate in, or intervene in (including the publishing or distribution of statements) any political campaign on behalf of or in opposition to any candidate for public office. Notwithstanding any other provision of these articles, the corporation shall not carry on any

other activities not permitted to be carried on (a) by a corporation exempt from federal income tax under section 501(c)(3) of the Internal Revenue Code, or the corresponding section of any future federal tax code, or (b) by a corporation, contributions to which are deductible under section 170(c)(2) of the Internal Revenue Code, or the corresponding section of any future federal tax code.

See Publication 557 for further information and examples of acceptable language that expressly limits you to engage in activities in furtherance of one or more exempt purposes described in section 501(c)(3).

TIP *See the instructions for Part III, later, for more information on activities that exclusively further one or more exempt purposes, and certain activities that are prohibited or restricted for organizations exempt from federal income tax under section 501(c)(3).*

Line 7. Dissolution clause. Your organizing document must permanently dedicate your assets for a section 501(c)(3) purpose. This means that if you dissolve your organization in the future, your assets must be distributed for an exempt purpose described in section 501(c)(3), or to the federal government, or to a state or local government, for a public purpose.

If your organizing document states that your assets would be distributed to members or private individuals or for any purpose other than those provided in section 501(c)(3), you must amend your organizing document to remove such statements before you apply for recognition of exemption.

The following is an example of an acceptable dissolution clause:

Upon the dissolution of this organization, assets shall be distributed for one or more exempt purposes within the meaning of section 501(c)(3) of the Internal Revenue Code, or corresponding section of any future federal tax code, or shall be distributed to the federal government, or to a state or local government, for a public purpose.

Naming a specific organization or organizations to receive your assets upon dissolution will be acceptable only if your articles state that the specific organization(s) must be exempt under section 501(c)(3) at the time your dissolution takes place and your organizing document provides for distribution for one or more exempt purposes within the meaning of section 501(c)(3) if the specific organization(s) are not exempt.

See Publication 557 for further information and examples of acceptable language for dedication of assets upon dissolution in your organizing document.

Operation of state law. The laws of certain states provide for the distribution of assets upon dissolution. Therefore, specific written language regarding distribution of assets upon dissolution may not be needed in the organizing documents of exempt organizations organized in those states. Organizations that are organized in these *cy pres* states should be aware of their specific state requirements. Operation of state law is based on Rev. Proc. 82-2, 1982-1 C.B. 367.

CAUTION *State law does not override an inappropriate dissolution clause. If you are organized in a* cy pres *state and do not have a dissolution clause, state law is sufficient to meet the dissolution clause. However, if you have an inappropriate dissolution clause (for example, a clause specifying that assets will or may be distributed to officers and/or directors upon dissolution), state law will not override this inappropriate clause, and you will need to amend your organizing document to remove the inappropriate clause before you apply for recognition of exemption.*

Part III. Your Specific Activities

Consider your past, present, and planned activities when responding to these questions.

Line 1. National Taxonomy of Exempt Entities (NTEE) code. An NTEE code is a three-character series of letters and numbers that generally summarize an organization's purpose. Enter the code that best describes your organization from the list of NTEE codes, later, in these instructions. For more information and more detailed definitions of these codes developed by the National Center for Charitable Statistics (NCCS), visit the Urban Institute, NCCS website at *www.nccsdataweb.urban.org*.

Note. NTEE codes are also used for purposes other than identification of organizations described in section 501(c)(3). Therefore, all codes in the list do not necessarily describe a 501(c)(3) purpose. Selecting the appropriate NTEE code is important as some donors use the codes to identify potential recipients of grants.

Line 2. Exempt purposes. In order to qualify for exemption as an organization described in section 501(c)(3), you must be organized and operated exclusively for one or more of the following purposes: charitable, religious, educational, scientific, literary, testing for public safety, fostering national or international amateur sports competition, or preventing cruelty to children or animals. An organization is not regarded as being organized and operated exclusively for exempt purposes if more than an insubstantial part of its activities is not in furtherance of an exempt purpose. For more information, see Publication 557.

Note. An organization does not qualify for exemption as an organization described in section 501(c)(3) if its purposes are illegal or contrary to public policy. See Rev. Rul. 71-447, 1971-2 C.B. 230 (a private school that does not have a racially nondiscriminatory policy as to students does not qualify for exemption). Furthermore, an organization operated for the primary purpose of carrying on a trade or business for profit shall not be exempt from taxation under section 501(c)(3), even if all of its profits are payable to one or more organizations exempt from taxation under section 501.

Charitable. The generally accepted legal definition of "charitable" includes relief of the poor, the distressed, or the underprivileged; advancement of religion; advancement of education or science; erecting or maintaining public buildings, monuments, or works; lessening the burdens of government; lessening neighborhood tensions; eliminating prejudice and discrimination; defending human and civil rights secured by law; and combating community deterioration and juvenile delinquency.

Religious. To determine whether an organization meets the religious purposes test of section 501(c)(3), the IRS maintains two basic guidelines.

1. That the particular religious beliefs of the organization are truly and sincerely held. If there is a clear showing that the beliefs (or doctrines) are sincerely held by those professing them, the IRS will not question the religious nature of those beliefs.
2. That the practices and rituals associated with the organization's religious belief or creed are not illegal or contrary to clearly defined public policy. Therefore, an organization may not qualify for treatment as an exempt religious organization for tax purposes if its actions are contrary to well established and clearly defined public policy.

Educational. The term "educational," as used in section 501(c)(3), relates to:

- The instruction or training of the individual for the purpose of improving or developing his or her capabilities, or
- The instruction of the public on subjects useful to the individual and beneficial to the community.

An organization may be educational even though it advocates a particular position or viewpoint so long as it presents a sufficiently full and fair exposition of the pertinent facts as to permit an individual or the public to form an independent opinion or conclusion. On the other hand, an organization is not educational if its principal function is the mere presentation of unsupported opinion.

The term "educational" includes the provision of childcare away from the home if:

1. Substantially all of the care provided by the organization is to enable individuals (parents) to be gainfully employed, and
2. The services provided by the organization are available to the general public.

The following are examples of organizations which, if they otherwise meet the requirements of this section, are educational.

Example 1. An organization, such as a primary or secondary school, a college, or a professional or trade school, which has a regularly scheduled curriculum, a regular faculty, and a regularly enrolled body of students in attendance at a place where the educational activities are regularly carried on.

Example 2. An organization whose activities consist of presenting public discussion groups, forums, panels, lectures, or other similar programs. Such programs may be on radio or television.

Example 3. An organization which presents a course of instruction by means of correspondence or through the utilization of television or radio.

Example 4. Museums, zoos, planetariums, symphony orchestras, and other similar organizations.

Scientific. To be a scientific organization under section 501(c)(3), an organization must be organized and operated in the public interest. Therefore, the term "scientific," as used in section 501(c)(3), includes the carrying on of scientific research in the public interest. Scientific research does not include activities of a type ordinarily carried on as an incident to commercial or industrial operations, as, for example, the ordinary testing or inspection of materials or products, or the designing or construction of equipment or buildings.

Scientific research will be regarded as carried on in the public interest if:

1. The results of such research (including any patents, copyrights, processes, or formulae resulting from such research) are made available to the public on a nondiscriminatory basis;
2. Such research is performed for the United States, or any of its agencies or instrumentalities, or for a State or political subdivision thereof; or
3. Such research is directed toward benefiting the public.

Testing for public safety. The term "testing for public safety," as used in section 501(c)(3), includes the testing of consumer products, such as electrical products, to determine whether they are safe for use by the general public.

To foster national or international amateur sports competition. There are two types of amateur athletic organizations that can qualify for tax-exempt status. The first type is an organization that fosters national or international amateur sports competition, but only if none of its activities involve providing athletic facilities or equipment. The second type is a qualified amateur sports organization under section 501(j) (discussed below). The primary difference between the two is that a qualified amateur sports organization can provide athletic facilities and equipment.

An organization will be a qualified amateur sports organization under section 501(j) if it is organized and operated:

1. Exclusively to foster national or international amateur sports competition, and
2. Primarily to conduct national or international competition in sports or to support and develop amateur athletes for that competition.

The organization's membership can be local or regional in nature.

Prevention of cruelty to children or animals. Examples of activities that may qualify this type of organization for exempt status are:

1. Preventing children from working in hazardous trades or occupations,
2. Promoting high standards of care for laboratory animals, and
3. Providing funds to pet owners to have their pets spayed or neutered to prevent over-breeding.

Line 3. Prohibited or restricted activities. Certain activities are prohibited or restricted for organizations exempt from federal income tax under section 501(c)(3). Along with conducting activities that exclusively further one or more of the purposes listed in Part III, line 2, earlier, organizations exempt under section 501(c)(3) must:

a) Refrain from supporting or opposing candidates in political campaigns in any way.

An organization exempt under section 501(c)(3) is prohibited from directly or indirectly participating in, or intervening in, any political campaign on behalf of (or in opposition to) any candidate for elective public office. The prohibition applies to all campaigns, including campaigns at the federal, state, and local level.

Political campaign intervention includes any and all activities that favor or oppose one or more candidates for public office. The prohibition extends beyond candidate endorsements. Contributions to political campaign funds or public statements of position (verbal or written) made by or on behalf of an organization in favor of or in opposition to any candidate for public office clearly violate the prohibition on political campaign intervention. Distributing statements prepared by others that favor or oppose any candidate for public office will also violate the prohibition. Allowing a candidate to use an organization's assets or facilities will also violate the prohibition if other candidates are not given an equivalent opportunity.

Certain activities will require an evaluation of all the facts and circumstances to determine whether they result in political campaign intervention. For example, section 501(c)(3) organizations are permitted to conduct certain voter education activities (including the presentation of public forums and the publication of voter education guides) if they are carried out in a non-partisan manner. In addition, section 501(c)(3) organizations may encourage people to participate in the electoral process through voter registration and get-out-the-vote drives conducted in a non-partisan manner. On the other hand, voter education or registration activities conducted in a biased manner that favors (or opposes) one or more candidates is prohibited.

For examples of relevant facts and circumstances, see Rev. Rul. 2007-41, 2007-1 C.B. 1421.

b) Ensure that net earnings do not inure in whole or in part to the benefit of private shareholders or individuals (that is, board members, officers, key management employees, or other insiders).

An organization is not operated exclusively for one or more exempt purposes if its net earnings inure in whole or in part to the benefit of private shareholders or individuals. The term "private shareholder or individual" refers to persons who have a personal and private interest in the organization, such as an officer, director, or a key employee. Any amount of inurement may be grounds for loss of tax-exempt status.

Note. Examples of inurement include the payment of dividends and the payment of unreasonable compensation to private shareholders or individuals.

c) Not further non-exempt purposes (such as purposes that benefit private interests) more than insubstantially.

An organization cannot conduct activities that further any purposes other than those described in Part III, line 2 of these instructions more than insubstantially, including benefitting private interests rather than the public as a whole. For example, an organization whose sole activity is the operation of a scholarship program for making payments to pre-selected, specifically named individuals is serving private interests rather than public interests. See Rev. Rul. 67-367, 1967-2 C.B. 188.

d) Not be organized or operated for the primary purpose of conducting a trade or business that is unrelated to exempt purpose(s).

An activity is an unrelated trade or business (and subject to unrelated business income tax) if it meets three requirements.

1. It is a trade or business.
2. It is regularly carried on.
3. It is not substantially related to furthering the exempt purpose(s) of the organization.

Trade or business. The term "trade or business" generally includes any activity conducted for the production of income from selling goods or performing services. An activity does not lose its identity as a trade or business merely because it is conducted within a larger group of similar activities that may or may not be related to the exempt purposes of the organization.

Regularly carried on. Business activities of an exempt organization ordinarily are considered regularly conducted if they show a frequency and continuity similar to, and are pursued in a manner similar to, comparable commercial activities of nonexempt organizations.

Not substantially related. A business activity is not substantially related to an organization's exempt purpose if it does not contribute importantly to accomplishing that purpose (other than through the production of funds). Whether an activity contributes importantly depends in each case on the facts involved.

For more information, see Publication 598.

e) Not devote more than an insubstantial part of activities to attempting to influence legislation.

In general, if a substantial part of an organization's activities consists of carrying on propaganda or otherwise attempting to influence legislation, it does not qualify for exemption under section 501(c)(3).

Legislation includes action by Congress, any state legislature, any local council, or similar governing body, with respect to acts, bills, resolutions, or similar items (such as legislative confirmation of appointive office), or by the public in referendum, ballot initiative, constitutional amendment, or similar procedure. It does not include actions by executive, judicial, or administrative bodies.

An organization will be regarded as attempting to influence legislation if it contacts, or urges the public to contact, members or employees of a legislative body for the purpose of proposing, supporting, or opposing legislation, or if the organization advocates the adoption or rejection of legislation.

TIP *Most public charities are eligible to elect under section 501(h) to have their legislative activities measured solely by an expenditure limit rather than by the "no substantial amount" limit. An election is made by filing Form 5768, Election/Revocation of Election by an Eligible Section 501(c)(3) Organization To Make Expenditures To Influence Legislation. If you are eligible and would like to make the election, file Form 5768. Private foundations cannot make this election.*

For additional information on the expenditure limit or the no substantial amount limit, see *www.irs.gov/Charities-&-Non-Profits/Lobbying*.

f) Not provide commercial-type insurance as a substantial part of activities.

An organization described in section 501(c)(3) shall be exempt from tax only if no substantial part of its activities consists of providing commercial-type insurance. The term "commercial-type insurance" does not include:

- Insurance provided at substantially below cost to a class of charitable recipients,
- Incidental health insurance provided by a health maintenance organization of a kind customarily provided by such organizations,
- Property or casualty insurance provided (directly or through an organization described in section 414(e)(3)(B)(ii)) by a church or convention or association of churches for such church or convention or association of churches,
- Providing retirement or welfare benefits (or both) by a church or a convention or association of churches (directly or through an organization described in section 414(e)(3)(A) or 414(e)(3)(B)(ii)) for the employees (including employees described in section 414(e)(3)(B)) of such church or convention or association of churches or the beneficiaries of such employees, and
- Charitable gift annuities.

Line 4. Attempting to influence legislation. Check "Yes" if you have attempted, or plan to attempt, to influence legislation. See the instructions for Part III, line 3, earlier, for a description of "attempting to influence legislation."

Line 5. Compensation to officers, directors, or trustees. Check "Yes" if you pay or plan to pay compensation to any of your officers, directors, or trustees.

Compensation includes salary or wages, deferred compensation, retirement benefits whether in the form of a qualified or non-qualified employee plan (pensions or annuities), fringe benefits (personal vehicle, meals, lodging, personal and family educational benefits, low interest loans, payment of personal travel, entertainment, or other expenses, athletic or country club membership, personal use of your property), and bonuses.

Line 6. Donation of funds or payment of expenses to individuals. Check "Yes" if you have donated funds to or paid expenses for individual(s), or plan to donate funds to or pay expenses for individual(s) (other than paying for or reimbursing employees' business expenses).

An organization is not organized or operated exclusively for one or more exempt purposes unless it serves a public rather than a private interest. You do not qualify as tax-exempt if you are organized or operated for the benefit of private interests such as designated individuals, the creator or his or her family, or shareholders of the organization. For example, you may not set up a scholarship program to pay for the education expenses of a designated individual, such as a contributor's family member. See Rev. Rul. 67-367, 1967-2 C.B. 188.

Line 7. Conducting activities or providing grants outside the United States. Check "Yes" if you have conducted or plan to conduct activities outside the United States, or have provided or plan to provide grants or other assistance to individual(s) or organization(s) outside the United States. For purposes of this question, "outside the United States" means those locations other than the United States, its territories, and possessions.

Line 8. Financial transactions with officers, directors, or trustees. Check "Yes" if you have engaged in or plan to engage in financial transactions (for example, loans, grants, or other assistance, payments for goods or services, rents, etc.) with any of your officers, directors, or trustees, or any entities they own or control. (See the glossary in the Form 990 instructions for a definition of "control.")

Line 9. Unrelated business gross income. Check "Yes" if you have received or plan to receive unrelated business gross income of $1,000 or more during a tax year. Exempt organizations that receive unrelated business gross income of $1,000 or more during a tax year must file Form 990-T, Exempt Organization Business Income Tax Return. For more information, see Publication 598.

Line 10. Gaming activities. Check "Yes" if you have conducted or plan to conduct bingo or other gaming activities. For more information, see Publication 3079, Tax-Exempt Organizations and Gaming.

Line 11. Disaster relief assistance. Check "Yes" if you have provided or plan to provide disaster relief. For more information, see Publication 3833, Disaster Relief: Providing Assistance Through Charitable Organizations.

Because of the requirement that exempt organizations must serve a charitable class, you do not qualify as a tax-exempt disaster relief or emergency hardship organization if you provide assistance only to specific individuals, such as a few persons injured in a particular natural disaster. Similarly, donors cannot earmark contributions to a charitable organization for a particular individual or family.

Part IV. Foundation Classification

Organizations that are described in section 501(c)(3) are classified as either public charities or private foundations. A public charity generally has a broad base of support, while a private foundation generally receives its support from a small number of donors. This classification is important because different tax rules apply to the operations of each entity. Deductibility of contributions to a private foundation is more limited than contributions to a public charity. See Publication 526, Charitable Contributions, for more information on the deductibility of contributions. In addition, as described below, private foundations are subject to excise taxes that are not imposed on public charities.

To be classified as a public charity, a section 501(c)(3) organization must meet one of the exceptions to private foundation status described in section 509(a)(1), 509(a)(2), 509(a)(3), or 509(a)(4). For a description of the categories of public charities, see Publication 557.

All other section 501(c)(3) organizations are classified as private foundations. Some private foundations are private operating foundations. Additional information about private foundations and private operating foundations is available in Publication 4221-PF, Compliance Guide for 501(c)(3) Private Foundations, and at *www.irs.gov/Charities-&-Non-Profits/Private-Foundations/Private-Operating-Foundations*.

Note. Many organizations described in section 501(c)(3) meet one of the exceptions described above and are classified as public charities, which are subject to more favorable treatment under tax law than are private foundations.

Private operating foundations and certain categories of public charities, such as churches, schools, and hospitals, are not eligible to apply for exemption under section 501(c)(3) using Form 1023-EZ. To determine if you are eligible to file Form 1023-EZ, complete the Form 1023-EZ Eligibility Worksheet, later.

Organizations that are eligible to apply for exemption using Form 1023-EZ and meet the requirements of section 501(c)(3) are private foundations *unless* they:

- Have broad financial support from the general public (as described in the instructions for **Lines 1a** and **1b** below), or
- Are operated for the benefit of a college or university that is owned or operated by a governmental unit (as described in the instructions for **Line 1c** below).

Unless you meet one of these exceptions, you are a private foundation and must complete **Line 2**.

If you meet one of the exceptions above, you must select your public charity status in **Line 1**. **You may only check one box in Line 1.**

Line 1a. Check this box if you either:

- Normally receive 33⅓% or more of your total support from governmental agencies, contributions from the general public, and contributions or grants from other public charities (the "33⅓% public support test"); or
- Satisfy the following three-part "facts and circumstances test": (1) you normally receive 10% or more of your total support from governmental agencies, contributions from the general public, and contributions or grants from other public charities (the "10% public support requirement"); (2) you are organized and operated to attract new and additional public or governmental support on a continuous basis (the attraction of public support requirement); and (3) you have other characteristics of a publicly supported organization (see other factors below).

Facts and circumstances test: other factors. The following factors are taken into account in determining whether an organization that meets the 10% public support requirement and the attraction of public support requirement qualifies as publicly supported: (i) the percentage of financial support the organization receives from the general public, governmental units, or public charities (the higher the percentage, the lower the burden of meeting the other factors); (ii) whether the organization receives support from a representative number of persons; and (iii) all other facts and circumstances, including the public nature of the organization's governing body, the extent to which its facilities or programs are publicly available, the extent to which its dues encourage membership, and whether its activities are likely to appeal to persons having a broad common interest or purpose. For additional information about the facts and circumstances test, see Publication 557, and Regulations section 1.170A-9(f)(3).

The following definitions apply for purposes of both the 33⅓% public support test and the 10% public support requirement.

Normally. Whether an organization "normally" receives the required level of public support generally is measured using a

five-year computation period that includes the current tax year and four prior tax years. For a newly formed organization, the test is whether the organization can reasonably be expected to meet the requirements of the 33⅓% public support test or the 10% public support plus facts and circumstances test during its first five taxable years as a section 501(c)(3) organization. The basic consideration is whether its organizational structure, current or proposed programs or activities, and actual or intended method of operation can reasonably be expected to attract the type of broadly based support from the general public, public charities, and governmental units that is necessary to meet the public support requirements described above. For more information about the public support requirements, see Publication 557.

Total support. "Total support" includes contributions, membership fees, net income from unrelated business activities, and gross investment income, but does not include income from activities directly related to your exempt function.

Public support. "Public support" does not include contributions from any individual, corporation, or trust that exceed 2% of the organization's total support during the five-year computation period. In applying the 2% limit, all contributions made by a donor and by any persons in a special relationship to the donor (for example, family members of the donor and entities controlled by the donor) are considered made by one person.

Note. You do not meet either of these public support tests if you receive almost all of your support from gross receipts from related activities and an insignificant amount of your support from governmental units and contributions made directly or indirectly by the general public.

Line 1b. Check this box if you normally receive (1) more than 33⅓% of your support from contributions, membership fees, and gross receipts (from permitted sources, see below) from admissions, sales of merchandise, performance of services, or furnishing of facilities in an activity that is not an unrelated trade or business, subject to certain limits described below; and (2) not more than 33⅓% of your support from gross investment income and net unrelated business income (less the amount of tax on unrelated business taxable income under section 511).

For this purpose, "permitted sources" are governmental units, public charities described in section 509(a)(1), and persons other than disqualified persons. For additional information, see Publication 557.

Gross receipts from permitted sources. Gross receipts from related activities received from a person or from any government agency are includible in any tax year only to the extent the gross receipts are not more than the greater of $5,000 or 1% of the organization's total support in that year.

Normally. Whether an organization "normally" meets these support tests generally is measured using a five-year computation period that includes the current tax year and four prior tax years. For a newly formed organization, the test is whether it can reasonably be expected to meet the 33⅓% support test and the not-more-than 33⅓% support test during its first five taxable years as a section 501(c)(3) organization. For factors considered in determining whether an organization can reasonably be expected to meet these tests, see Publication 557.

TIP *For help determining if you meet one of the two public support tests described above, complete Schedule A (Form 990 or 990-EZ), Public Charity Status and Public Support, Parts II and III.*

Line 1c. Check this box if you both (1) are organized and operated exclusively to receive, hold, invest, and administer property for and make expenditures to or for the benefit of a state or municipal college or university (see below); and (2) normally receive a substantial part of your support from a governmental unit or from direct or indirect contributions from the general public, or from a combination of these sources.

The college or university you benefit must be:

- An agency or instrumentality of a state or political subdivision,
- Owned and operated by a state or political subdivision, or
- Owned and operated by an agency or instrumentality of one or more states or political subdivisions.

For this purpose, "support" does not include income received in the exercise or performance by the organization of its charitable, educational, or other purpose or function constituting the basis for exemption. See Publication 557 for additional information.

Line 2. If you checked one of the boxes in **Line 1** because you meet one of the public charity exceptions, do not complete the rest of this section. If you are organized and operated exclusively for tax-exempt purposes under section 501(c)(3) but do not meet one of the public charity tests listed in **Lines 1a – 1c**, you are a private foundation and must complete **Line 2**.

As a private foundation you are not tax exempt unless your organizing document contains specific provisions required by section 508(e). These specific provisions require that you operate to avoid liability for excise taxes under sections 4941(d) (acts of self-dealing), 4942 (undistributed income), 4943(c) (excess business holdings), 4944 (jeopardizing investments), and 4945(d) (taxable expenditures). Additional information regarding these private foundation excise taxes is available in Publication 4221-PF, Compliance Guide for 501(c)(3) Private Foundations, and at *www.irs.gov/Charities-&-Non-Profits/Private-Foundations/Private-Foundation-Excise-Taxes*.

For samples of provisions that will meet the section 508(e) requirements, see Publication 557, Chapter 3, Section 501(c)(3) Organizations: Private Foundations.

Operation of state law. Some states have enacted statutory provisions that satisfy the requirements of section 508(e), subject to notations. Organizations that are organized in a state that has a statutory provision addressing the requirements of section 508(e) should be aware of their specific state requirements. Operation of state law is based on Rev. Rul. 75-38, 1975-1 C.B. 161.

Check **Line 2** to attest that either your organizing document contains the appropriate provisions or that the provisions are met by operation of state law.

Note. Private foundations are required to obtain advance approval from the IRS before making grants to individuals for travel, study, or similar purposes. Failure to do so will result in excise taxes under section 4945. Under section 4945, the excise tax does not apply to an individual grant awarded on an objective and nondiscriminatory basis pursuant to a procedure approved by the IRS in advance. Additional information regarding these rules is available at *www.irs.gov/Charities-&-Non-Profits/Private-Foundations/Grants-to-Individuals*.

To request advance approval of grantmaking procedures under section 4945(g) you must complete and submit Form 8940. A user fee must accompany the form. The advance approval request should be sent to the address indicated on Form 8940. It cannot be submitted with Form 1023-EZ. Additional information about advance approval of individual grant procedures is available at *www.irs.gov/Charities-&-Non-Profits/Private-Foundations/Advance-Approval-of-Grant-Making-Procedures*. Alternatively, if you do not wish to submit a Form 1023-EZ and a Form 8940, private foundations required to obtain advance approval may complete the full Form 1023 instead.

Part V. Reinstatement After Automatic Revocation

You should complete this section only if you have had your exempt status automatically revoked under section 6033(j)(1) of the Code for failure to file required annual returns or notices for three consecutive years, and you are applying for reinstatement under section 4 or 7 of Rev. Proc. 2014-11, 2014-3 I.R.B. 411.

Rev. Proc. 2014-11 establishes several different procedures for reinstating organizations depending upon their size, number of times they have been automatically revoked, and the timeliness of filing for reinstatement. Therefore, you should review the revenue procedure and determine which section applies to you.

Note. You can apply using this form only if you are requesting reinstatement under section 4 or 7 of the revenue procedure. If you are applying for retroactive reinstatement under section 5 or 6 of Rev. Proc. 2014-11, you must submit the full Form 1023 along with the appropriate reasonable cause statement and a statement confirming you have filed the required annual returns as described in the revenue procedure.

Line 1. Section 4 of Rev. Proc. 2014-11. Check this box if:

- You were eligible to file either Form 990-EZ or Form 990-N for each of the three consecutive years that you failed to file,
- This is the first time you have been automatically revoked pursuant to section 6033(j), and
- You are submitting this application not later than 15 months after the later of the date of your Revocation Letter or the date on which the IRS posted your name on the Revocation List at *www.irs.gov/Charities-&-Non-Profits/Exempt-Organizations-Select-Check*.

By checking this box, you are also attesting that your failure to file was not intentional and you have put in place procedures to file required returns or notices in the future.

Line 2. Section 7 of Rev. Proc. 2014-11. Check this box if you are seeking reinstatement under section 7 of Rev. Proc. 2014-11. By checking this box, you are agreeing to accept an effective date of reinstatement as of the date of filing this application.

Part VI. Signature

An officer, director, or trustee listed in Part I, line 8, who is authorized to sign for the organization must electronically sign Form 1023-EZ. To electronically sign Form 1023-EZ, the signer must check the "penalties of perjury" box in Part VI and type his or her name on the line provided. The signature must be accompanied by the title or authority of the signer and the date.

Paperwork Reduction Act Notice. The time needed to complete and file this form will vary depending on individual circumstances. The estimated average time is:

Recordkeeping	10 hr., 02 min.
Learning about the law or the form	2 hr., 30 min.
Preparing the form	5 hr., 33 min.
Copying, assembling, and sending the form to the IRS	48 min.

If you have comments concerning the accuracy of these time estimates or suggestions for making this form simpler, we would be happy to hear from you. You can send your comments to Internal Revenue Service, Tax Forms and Publications Division, 1111 Constitution Ave. NW, IR-6526, Washington, DC 20224. Do not send the tax form to this address. Instead, see How To File, earlier.

Form 1023-EZ Eligibility Worksheet
(Must be completed prior to completing Form 1023-EZ)

If you answer "Yes" to any of the worksheet questions, you are not eligible to apply for exemption under section 501(c)(3) using Form 1023-EZ. You must apply on Form 1023. If you answer "No" to all of the worksheet questions, you may apply using Form 1023-EZ.

1.	**Do you project that your annual gross receipts will exceed $50,000 in any of the next 3 years?** Gross receipts are the total amounts the organization received from all sources during its annual accounting period, without subtracting any costs or expenses. You should consider this year and the next two years.	☐ **Yes**	☐ **No**
2.	**Have your annual gross receipts exceeded $50,000 in any of the past 3 years?**	☐ **Yes**	☐ **No**
3.	**Do you have total assets the fair market value of which is in excess of $250,000?** Total assets includes cash, accounts receivable, inventories, bonds and notes receivable, corporate stocks, loans receivable, other investments, depreciable and depletable assets, land, buildings, equipment, and any other assets.	☐ **Yes**	☐ **No**
4.	**Were you formed under the laws of a foreign country (United States territories and possessions are not considered foreign countries)?** You are formed under the laws of a foreign country if you are not formed under the laws of (1) the United States, its states, territories, or possessions; (2) federally recognized Indian tribal or Alaskan native governments; or (3) the District of Columbia.	☐ **Yes**	☐ **No**
5.	**Is your mailing address in a foreign country (United States territories and possessions are not considered foreign countries)?** Your mailing address is the address where all correspondence will be sent.	☐ **Yes**	☐ **No**
6.	**Are you a successor to, or controlled by, an entity suspended under section 501(p) (suspension of tax-exempt status of terrorist organizations)?** Section 501(p)(1) suspends the exemption from tax under section 501(a) of any organization described in section 501(p)(2). An organization is described in section 501(p)(2) if the organization is designated or otherwise individually identified (1) under certain provisions of the Immigration and Nationality Act as a terrorist organization or foreign terrorist organization; (2) in or pursuant to an Executive Order which is related to terrorism and issued under the authority of the International Emergency Economic Powers Act or section 5 of the United Nations Participation Act of 1945 for the purpose of imposing on such organization an economic or other sanction; or (3) in or pursuant to an Executive Order issued under the authority of any federal law, if the organization is designated or otherwise individually identified in or pursuant to the Executive Order as supporting or engaging in terrorist activity (as defined in the Immigration and Nationality Act) or supporting terrorism (as defined in the Foreign Relations Authorization Act) and the Executive Order refers to section 501(p)(2). Under section 501(p)(3) of the Code, suspension of an organization's tax exemption begins on the date of the first publication of a designation or identification with respect to the organization, as described above, or the date on which section 501(p) was enacted, whichever is later. This suspension continues until all designations and identifications of the organization are rescinded under the law or Executive Order under which such designation or identification was made.	☐ **Yes**	☐ **No**

7.	**Are you organized as an entity other than a corporation, unincorporated association, or trust?** Answer "Yes" if you are organized as an LLC under the laws of the state in which you were formed.	☐ **Yes**	☐ **No**
8.	**Are you a successor to a for-profit entity?** You are a successor if you have: 1. Substantially taken over all of the assets or activities of a for-profit entity; 2. Been converted or merged from a for-profit entity; or 3. Installed the same officers, directors, or trustees as a for-profit entity that no longer exists.	☐ **Yes**	☐ **No**
9.	**Were you previously revoked or are you a successor to a previously revoked organization (other than an organization the tax-exempt status of which was automatically revoked for failure to file a Form 990-series return for three consecutive years)?** Do not check "Yes" if your previous revocation, or your predecessor's revocation, was an automatic revocation (pursuant to section 6033(j)) for failing to satisfy Form 990-series filing requirements for three consecutive years.	☐ **Yes**	☐ **No**
10.	**Are you a church or a convention or association of churches described in section 170(b)(1)(A)(i)?** There is no single definition of the word "church" for tax purposes; however, the characteristics generally attributed to churches include: • A distinct legal existence, • A recognized creed and form of worship, • A definite and distinct ecclesiastical government, • A formal code of doctrine and discipline, • A distinct religious history, • A membership not associated with any other church or denomination, • Ordained ministers ministering to the congregation, • Ordained ministers selected after completing prescribed courses of study, • A literature of its own, • Established places of worship, • Regular congregations, • Regular religious services, • Sunday schools for the religious instruction of the young, and • Schools for the preparation of ministers. Although it is not necessary that each of the above characteristics be present, a congregation or other religious membership group that meets regularly for religious worship is generally required. A church includes mosques, temples, synagogues, and other forms of religious organizations. For more information, see Publication 1828.	☐ **Yes**	☐ **No**

11.	**Are you a school, college, or university described in section 170(b)(1)(A)(ii)?** An organization is a school if it: 1. Presents formal instruction as its primary function, 2. Has a regularly scheduled curriculum, 3. Has a regular faculty of qualified teachers, 4. Has a regularly enrolled student body, and 5. Has a place where educational activities are regularly carried on. The term "school" includes primary, secondary, preparatory, high schools, colleges, and universities. It does not include organizations engaged in both educational and non-educational activities, unless the latter are merely incidental to the educational activities.	☐ **Yes**	☐ **No**
12.	**Are you a hospital or medical research organization described in section 170(b)(1)(A)(iii) or a hospital organization described in section 501(r)(2)(A)(i)?** An organization is a hospital described in section 170(b)(1)(A)(iii) if its principal purpose or function is providing medical or hospital care, or medical education or research. Medical care includes treatment of any physical or mental disability or condition, on an inpatient or outpatient basis. Thus, if an organization is a rehabilitation institution, outpatient clinic, or community mental health or drug treatment center, it is a hospital if its principal function is providing treatment services as described above. A hospital does not include convalescent homes, homes for children or the aged, or institutions whose principal purpose or function is to train handicapped individuals to pursue a vocation. An organization is a medical research organization described in section 170(b)(1)(A)(iii) if its principal purpose or function is the direct, continuous, and active conduct of medical research in conjunction with a hospital. The hospital with which the organization is affiliated must be described in section 501(c)(3), a federal hospital, or an instrumentality of a governmental unit, such as a municipal hospital. An organization is a hospital organization described in section 501(r)(2)(A)(i) if the organization operates a facility which is required by a state to be licensed, registered, or similarly recognized as a hospital.	☐ **Yes**	☐ **No**

13.	**Are you applying for exemption as a cooperative hospital service organization under section 501(e)?** A cooperative hospital service organization described in section 501(e) is organized and operated on a cooperative basis to provide its section 501(c)(3) hospital members one or more of the following activities. • Data processing. • Purchasing (including purchasing insurance on a group basis). • Warehousing. • Billing and collection (including purchasing patron accounts receivable on a recourse basis). • Food. • Clinical. • Industrial engineering. • Laboratory. • Printing. • Communications. • Record center. • Personnel (including selecting, testing, training, and educating personnel) services. A cooperative hospital service organization must also meet certain other requirements specified in section 501(e).	☐ **Yes**	☐ **No**
14.	**Are you applying for exemption as a cooperative service organization of operating educational organizations under section 501(f)?** An organization is a cooperative service organization of operating educational organizations if it is organized and operated solely to provide investment services to its members. Those members must be organizations described in section 170(b)(1)(A)(ii) or (iv) that are tax exempt under section 501(a) or whose income is excluded from taxation under section 115.	☐ **Yes**	☐ **No**

15.	**Are you applying for exemption as a qualified charitable risk pool under section 501(n)?** A qualified charitable risk pool is treated as organized and operated exclusively for charitable purposes. Check the appropriate box to indicate whether you are a charitable risk pool. A qualified charitable risk pool is an organization that: 1. Is organized and operated only to pool insurable risks of its members (not including risks related to medical malpractice) and to provide information to its members about loss control and risk management, 2. Consists only of members that are section 501(c)(3) organizations exempt from tax under section 501(a), 3. Is organized under state law authorizing this type of risk pooling, 4. Is exempt from state income tax (or will be after qualifying as a section 501(c)(3) organization), 5. Has obtained at least $1,000,000 in startup capital from nonmember charitable organizations, 6. Is controlled by a board of directors elected by its members, and 7. Is organized under documents requiring that: a. Each member be a section 501(c)(3) organization exempt from tax under section 501(a), b. Each member that receives a final determination that it no longer qualifies under section 501(c)(3) notify the pool immediately, and c. Each insurance policy issued by the pool provide that it will not cover events occurring after a final determination described in (b).	☐ **Yes**	☐ **No**

16.	**Are you requesting classification as a supporting organization under section 509(a)(3)?** A supporting organization (as defined in section 509(a)(3)) differs from the other types of public charities described in section 509. Instead of describing an organization that conducts a particular kind of activity or that receives financial support from the general public, section 509(a)(3) describes organizations that have established certain relationships in support of public charities described in section 509(a)(1) or 509(a)(2). Thus, an organization can qualify as a supporting organization (and not be classified as a private foundation) even though it may be funded by a single donor, family, or corporation. This kind of funding ordinarily would indicate private foundation status, but a section 509(a)(3) organization has limited purposes and activities, and gives up a significant degree of independence. A supporting organization is an organization that: 1. Is organized and operated exclusively for the benefit of, to perform the functions of, or to carry out the purposes of one or more specified organizations as described in section 509(a)(1) or 509(a)(2). These section 509(a)(1) and 509(a)(2) organizations are commonly called publicly supported organizations. 2. Has one of three types of relationships with one or more organizations described in section 509(a)(1) or 509(a)(2). It must be: a. Operated, supervised, or controlled by one or more section 509(a)(1) or 509(a)(2) organizations (Type I supporting organization); b. Supervised or controlled in connection with one or more section 509(a)(1) or 509(a)(2) organizations (Type II supporting organization); or c. Operated in connection with one or more section 509(a)(1) or 509(a)(2) organizations (Type III supporting organization). 3. Is not controlled directly or indirectly by disqualified persons (as defined in section 4946) other than foundation managers and other than one or more organizations described in section 509(a)(1) or 509(a)(2). See Publication 557 for more information.	☐ **Yes**	☐ **No**
17.	**Is a substantial purpose of your activities to provide assistance to individuals through credit counseling activities such as budgeting, personal finance, financial literacy, mortgage foreclosure assistance, or other consumer credit areas?** These activities involve the education of the consumer on budgeting, personal finance, financial literacy, mortgage foreclosure assistance, or other consumer credit areas. It may also involve assisting the consumer in consolidating debt and negotiating between debtors and creditors to lower interest rates and waive late and over-limit fees.	☐ **Yes**	☐ **No**
18.	**Do you or will you invest 5% or more of your total assets in securities or funds that are not publicly traded?**	☐ **Yes**	☐ **No**
19.	**Do you participate, or intend to participate, in partnerships (including entities or arrangements treated as partnerships for federal tax purposes) in which you share losses with partners other than section 501(c)(3) organizations?**	☐ **Yes**	☐ **No**
20.	**Do you sell, or intend to sell carbon credits or carbon offsets?**	☐ **Yes**	☐ **No**
21.	**Are you a Health Maintenance Organization (HMO)?**	☐ **Yes**	☐ **No**

22.	**Are you an Accountable Care Organization (ACO), or an organization that engages in, or intends to engage in, ACO activities (such as participation in the Medicare Shared Savings Program (MSSP) or in activities unrelated to the MSSP described in Notice 2011–20, 2011–16 I.R.B. 652)?** ACOs are entities formed by groups of physicians, hospitals, and other health care service providers and suppliers to manage and coordinate the care provided to patients. For a discussion of tax law issues relating to ACOs, see Notice 2011-20 and FS-2011-11, available at *www.irs.gov/uac/Tax-Exempt-Organizations-Participating-in-the-Medicare-Shared-Savings-Program-through-Accountable-Care-Organizations*.	☐ **Yes**	☐ **No**
23.	**Do you maintain or intend to maintain one or more donor advised funds?** In general, a donor advised fund is a fund or account that is owned and controlled by the organization but that is separately identified by reference to contributions of a donor or donors and with respect to which a donor (or any person appointed or designated by the donor) has or expects to have advisory privileges concerning the distribution or investment of amounts held in the fund or account by reason of the donor's status as a donor. For additional information, see Publication 557. Check "No" if you are a governmental unit referred to in section 170(c)(1) or a private foundation referred to in section 509(a).	☐ **Yes**	☐ **No**
24.	**Are you organized and operated exclusively for testing for public safety and requesting a foundation classification under section 509(a)(4)?** Generally, these organizations test consumer products to determine their acceptability for use by the general public.	☐ **Yes**	☐ **No**
25.	**Are you requesting classification as a private operating foundation?** Private foundations lack general public support. What distinguishes a private operating foundation from other private foundations is that it engages directly in the active conduct of charitable, religious, educational, and similar activities (as opposed to indirectly carrying out these activities by providing grants to individuals or other organizations). Private operating foundations are subject to more favorable rules than other private foundations in terms of charitable contribution deductions and attracting grants from private foundations. However, to be classified as a private operating foundation, an organization must meet certain tests. Additional information about private operating foundations is available at *www.irs.gov/Charities-&-Non-Profits/Private-Foundations/Private-Operating-Foundations*.	☐ **Yes**	☐ **No**
26.	**Are you applying for retroactive reinstatement of exemption under section 5 or 6 of Rev. Proc. 2014-11, after being automatically revoked?** Only organizations applying for reinstatement under section 4 or 7 of Rev. Proc. 2014-11 may use Form 1023-EZ. If you are applying for retroactive reinstatement under section 5 or 6 of Rev. Proc. 2014-11, you must submit the full Form 1023 along with the appropriate reasonable cause statement and a statement confirming you have filed the required annual returns as described in the revenue procedure.	☐ **Yes**	☐ **No**

National Taxonomy of Exempt Entities (NTEE) Codes.

Arts, Culture, and Humanities

A01	Alliance/Advocacy Organizations
A02	Management & Technical Assistance
A03	Professional Societies, Associations
A05	Research Institutes and/or Public Policy Analysis
A11	Single Organization Support
A12	Fund Raising and/or Fund Distribution
A19	Nonmonetary Support N.E.C.*
A20	Arts, Cultural Organizations - Multipurpose
A23	Cultural, Ethnic Awareness
A25	Arts Education
A26	Arts Council/Agency
A30	Media, Communications Organizations
A31	Film, Video
A32	Television
A33	Printing, Publishing
A34	Radio
A40	Visual Arts Organizations
A50	Museum, Museum Activities
A51	Art Museums
A52	Children's Museums
A54	History Museums
A56	Natural History, Natural Science Museums
A57	Science and Technology Museums
A60	Performing Arts Organizations
A61	Performing Arts Centers
A62	Dance
A63	Ballet
A65	Theater
A68	Music
A69	Symphony Orchestras
A6A	Opera
A6B	Singing, Choral
A6C	Music Groups, Bands, Ensembles
A6E	Performing Arts Schools
A70	Humanities Organizations
A80	Historical Societies, Related Historical Activities
A84	Commemorative Events
A90	Arts Service Organizations and Activities
A99	Arts, Culture, and Humanities N.E.C.

Education

B01	Alliance/Advocacy Organizations
B02	Management & Technical Assistance
B03	Professional Societies, Associations
B05	Research Institutes and/or Public Policy Analysis
B11	Single Organization Support
B12	Fund Raising and/or Fund Distribution
B19	Nonmonetary Support N.E.C.
B20	Elementary, Secondary Education, K - 12
B21	Kindergarten, Preschool, Nursery School, Early Admissions
B24	Primary, Elementary Schools
B25	Secondary, High School
B28	Specialized Education Institutions
B30	Vocational, Technical Schools
B40	Higher Education Institutions
B41	Community or Junior Colleges
B42	Undergraduate College (4-year)
B43	University or Technological Institute
B50	Graduate, Professional Schools (Separate Entities)
B60	Adult, Continuing Education
B70	Libraries
B80	Student Services, Organizations of Students
B82	Scholarships, Student Financial Aid Services, Awards
B83	Student Sororities, Fraternities
B84	Alumni Associations
B90	Educational Services and Schools - Other
B92	Remedial Reading, Reading Encouragement
B94	Parent/Teacher Group
B99	Education N.E.C.

Environmental Quality, Protection, and Beautification

C01	Alliance/Advocacy Organizations
C02	Management & Technical Assistance
C03	Professional Societies, Associations
C05	Research Institutes and/or Public Policy Analysis
C11	Single Organization Support
C12	Fund Raising and/or Fund Distribution
C19	Nonmonetary Support N.E.C.
C20	Pollution Abatement and Control Services
C27	Recycling Programs
C30	Natural Resources Conservation and Protection
C32	Water Resource, Wetlands Conservation and Management
C34	Land Resources Conservation
C35	Energy Resources Conservation and Development
C36	Forest Conservation
C40	Botanical, Horticultural, and Landscape Services
C41	Botanical Gardens, Arboreta and Botanical Organizations
C42	Garden Club, Horticultural Program
C50	Environmental Beautification and Aesthetics
C60	Environmental Education and Outdoor Survival Programs
C99	Environmental Quality, Protection, and Beautification N.E.C.

Animal-Related

D01	Alliance/Advocacy Organizations
D02	Management & Technical Assistance
D03	Professional Societies, Associations
D05	Research Institutes and/or Public Policy Analysis
D11	Single Organization Support
D12	Fund Raising and/or Fund Distribution
D19	Nonmonetary Support N.E.C.
D20	Animal Protection and Welfare
D30	Wildlife Preservation, Protection
D31	Protection of Endangered Species
D32	Bird Sanctuary, Preserve
D33	Fisheries Resources
D34	Wildlife Sanctuary, Refuge
D40	Veterinary Services
D50	Zoo, Zoological Society
D60	Other Services - Specialty Animals
D61	Animal Training, Behavior
D99	Animal-Related N.E.C.

Health - General and Rehabilitative

E01	Alliance/Advocacy Organizations
E02	Management & Technical Assistance
E03	Professional Societies, Associations
E05	Research Institutes and/or Public Policy Analysis
E11	Single Organization Support
E12	Fund Raising and/or Fund Distribution
E19	Nonmonetary Support N.E.C.
E20	Hospitals and Related Primary Medical Care Facilities
E21	Community Health Systems
E22	Hospital, General
E24	Hospital, Specialty
E30	Health Treatment Facilities, Primarily Outpatient
E31	Group Health Practice (Health Maintenance Organizations)
E32	Ambulatory Health Center, Community Clinic
E40	Reproductive Health Care Facilities and Allied Services
E42	Family Planning Centers
E50	Rehabilitative Medical Services
E60	Health Support Services
E61	Blood Supply Related
E62	Ambulance, Emergency Medical Transport Services
E65	Organ and Tissue Banks
E70	Public Health Program (Includes General Health and Wellness Promotion Services)
E80	Health, General and Financing
E86	Patient Services - Entertainment, Recreation
E90	Nursing Services (General)
E91	Nursing, Convalescent Facilities
E92	Home Health Care
E99	Health - General and Rehabilitative N.E.C.

Mental Health, Crisis Intervention

F01	Alliance/Advocacy Organizations
F02	Management & Technical Assistance
F03	Professional Societies, Associations
F05	Research Institutes and/or Public Policy Analysis
F11	Single Organization Support
F12	Fund Raising and/or Fund Distribution
F19	Nonmonetary Support N.E.C.
F20	Alcohol, Drug and Substance Abuse, Dependency Prevention and Treatment
F21	Alcohol, Drug Abuse, Prevention Only
F22	Alcohol, Drug Abuse, Treatment Only
F30	Mental Health Treatment - Multipurpose and N.E.C.
F31	Psychiatric, Mental Health Hospital
F32	Community Mental Health Center
F33	Group Home, Residential Treatment Facility - Mental Health Related
F40	Hot Line, Crisis Intervention Services
F42	Rape Victim Services
F50	Addictive Disorders N.E.C.
F52	Smoking Addiction
F53	Eating Disorder, Addiction
F54	Gambling Addiction
F60	Counseling, Support Groups
F70	Mental Health Disorders
F80	Mental Health Association, Multipurpose
F99	Mental Health, Crisis Intervention N.E.C.

Diseases, Disorders, Medical Disciplines

G01	Alliance/Advocacy Organizations
G02	Management & Technical Assistance
G03	Professional Societies, Associations
G05	Research Institutes and/or Public Policy Analysis
G11	Single Organization Support
G12	Fund Raising and/or Fund Distribution
G19	Nonmonetary Support N.E.C.
G20	Birth Defects and Genetic Diseases
G25	Down Syndrome
G30	Cancer
G40	Diseases of Specific Organs
G41	Eye Diseases, Blindness and Vision Impairments
G42	Ear and Throat Diseases
G43	Heart and Circulatory System Diseases, Disorders
G44	Kidney Disease
G45	Lung Disease
G48	Brain Disorders
G50	Nerve, Muscle and Bone Diseases
G51	Arthritis
G54	Epilepsy
G60	Allergy Related Diseases G61 Asthma
G70	Digestive Diseases, Disorders
G80	Specifically Named Diseases
G81	AIDS
G83	Alzheimer's Disease
G84	Autism
G90	Medical Disciplines
G92	Biomedicine, Bioengineering
G94	Geriatrics
G96	Neurology, Neuroscience
G98	Pediatrics
G9B	Surgery
G99	Diseases, Disorders, Medical Disciplines N.E.C.

Medical Research

H01	Alliance/Advocacy Organizations
H02	Management & Technical Assistance
H03	Professional Societies, Associations
H05	Research Institutes and/or Public Policy Analysis
H11	Single Organization Support
H12	Fund Raising and/or Fund Distribution
H19	Nonmonetary Support N.E.C.
H20	Birth Defects, Genetic Diseases Research
H25	Down Syndrome Research
H30	Cancer Research
H40	Specific Organ Research
H41	Eye Research
H42	Ear and Throat Research
H43	Heart, Circulatory Research
H44	Kidney Research
H45	Lung Research
H48	Brain Disorders Research
H50	Nerve, Muscle, Bone Research
H51	Arthritis Research
H54	Epilepsy Research
H60	Allergy Related Disease Research
H61	Asthma Research
H70	Digestive Disease, Disorder Research
H80	Specifically Named Diseases Research
H81	AIDS Research
H83	Alzheimer's Disease Research
H84	Autism Research
H90	Medical Specialty Research
H92	Biomedicine, Bioengineering Research
H94	Geriatrics Research
H96	Neurology, Neuroscience Research
H98	Pediatrics Research
H9B	Surgery Research
H99	Medical Research N.E.C.

Crime, Legal Related

I01	Alliance/Advocacy Organizations
I02	Management & Technical Assistance
I03	Professional Societies, Associations
I05	Research Institutes and/or Public Policy Analysis

I11	Single Organization Support
I12	Fund Raising and/or Fund Distribution
I19	Nonmonetary Support N.E.C.
I20	Crime Prevention N.E.C.
I21	Delinquency Prevention
I23	Drunk Driving Related
I30	Correctional Facilities N.E.C.
I31	Transitional Care, Half-Way House for Offenders, Ex-Offenders
I40	Rehabilitation Services for Offenders
I43	Services to Prisoners and Families - Multipurpose
I44	Prison Alternatives
I50	Administration of Justice, Courts
I51	Dispute Resolution, Mediation Services
I60	Law Enforcement Agencies (Police Departments)
I70	Protection Against, Prevention of Neglect, Abuse, Exploitation
I71	Spouse Abuse, Prevention of
I72	Child Abuse, Prevention of
I73	Sexual Abuse, Prevention of
I80	Legal Services
I83	Public Interest Law, Litigation
I99	Crime, Legal Related N.E.C.

Employment, Job Related

J01	Alliance/Advocacy Organizations
J02	Management & Technical Assistance
J03	Professional Societies, Associations
J05	Research Institutes and/or Public Policy Analysis
J11	Single Organization Support
J12	Fund Raising and/or Fund Distribution
J19	Nonmonetary Support N.E.C.
J20	Employment Procurement Assistance, Job Training
J21	Vocational Counseling, Guidance and Testing
J22	Vocational Training
J30	Vocational Rehabilitation
J32	Goodwill Industries
J33	Sheltered Remunerative Employment, Work Activity Center N.E.C.
J40	Labor Unions, Organizations
J99	Employment, Job Related N.E.C.

Food, Agriculture, and Nutrition

K01	Alliance/Advocacy Organizations
K02	Management & Technical Assistance
K03	Professional Societies, Associations
K05	Research Institutes and/or Public Policy Analysis
K11	Single Organization Support
K12	Fund Raising and/or Fund Distribution
K19	Nonmonetary Support N.E.C.
K20	Agricultural Programs
K25	Farmland Preservation
K26	Livestock Breeding, Development, Management
K28	Farm Bureau, Grange
K30	Food Service, Free Food Distribution Programs
K31	Food Banks, Food Pantries
K34	Congregate Meals
K35	Eatery, Agency, Organization Sponsored
K36	Meals on Wheels
K40	Nutrition Programs
K50	Home Economics
K99	Food, Agriculture, and Nutrition N.E.C.

Housing, Shelter

L01	Alliance/Advocacy Organizations
L02	Management & Technical Assistance
L03	Professional Societies, Associations
L05	Research Institutes and/or Public Policy Analysis
L11	Single Organization Support
L12	Fund Raising and/or Fund Distribution
L19	Nonmonetary Support N.E.C.
L20	Housing Development, Construction, Management
L21	Public Housing Facilities
L22	Senior Citizens' Housing/ Retirement Communities
L25	Housing Rehabilitation
L30	Housing Search Assistance
L40	Low-Cost Temporary Housing
L41	Homeless, Temporary Shelter For
L50	Housing Owners, Renters Organizations
L80	Housing Support Services -- Other
L81	Home Improvement and Repairs
L82	Housing Expense Reduction Support
L99	Housing, Shelter N.E.C.

Public Safety, Disaster Preparedness, and Relief

M01	Alliance/Advocacy Organizations
M02	Management & Technical Assistance
M03	Professional Societies, Associations
M05	Research Institutes and/or Public Policy Analysis
M11	Single Organization Support
M12	Fund Raising and/or Fund Distribution
M19	Nonmonetary Support N.E.C.
M20	Disaster Preparedness and Relief Services
M23	Search and Rescue Squads, Services
M24	Fire Prevention, Protection, Control
M40	Safety Education
M41	First Aid Training, Services
M42	Automotive Safety
M99	Public Safety, Disaster Preparedness, and Relief N.E.C.

Recreation, Sports, Leisure, Athletics

N01	Alliance/Advocacy Organizations
N02	Management & Technical Assistance
N03	Professional Societies, Associations
N05	Research Institutes and/or Public Policy Analysis
N11	Single Organization Support
N12	Fund Raising and/or Fund Distribution
N19	Nonmonetary Support N.E.C.
N20	Recreational and Sporting Camps
N30	Physical Fitness and Community Recreational Facilities
N31	Community Recreational Centers
N32	Parks and Playgrounds
N40	Sports Training Facilities, Agencies
N50	Recreational, Pleasure, or Social Club
N52	Fairs, County and Other
N60	Amateur Sports Clubs, Leagues, N.E.C.
N61	Fishing, Hunting Clubs
N62	Basketball
N63	Baseball, Softball
N64	Soccer Clubs, Leagues
N65	Football Clubs, Leagues
N66	Tennis, Racquet Sports Clubs, Leagues
N67	Swimming, Water Recreation
N68	Winter Sports (Snow and Ice)
N69	Equestrian, Riding
N6A	Golf
N70	Amateur Sports Competitions
N71	Olympics Committees and Related International Competitions
N72	Special Olympics
N80	Professional Athletic Leagues
N99	Recreation, Sports, Leisure, Athletics N.E.C.

Youth Development

O01	Alliance/Advocacy Organizations
O02	Management & Technical Assistance
O03	Professional Societies, Associations
O05	Research Institutes and/or Public Policy Analysis
O11	Single Organization Support
O12	Fund Raising and/or Fund Distribution
O19	Nonmonetary Support N.E.C.
O20	Youth Centers, Clubs, Multipurpose
O21	Boys Clubs
O22	Girls Clubs O23 Boys and Girls Clubs (Combined)
O30	Adult, Child Matching Programs
O31	Big Brothers, Big Sisters
O40	Scouting Organizations
O41	Boy Scouts of America
O42	Girl Scouts of the U.S.A.
O43	Camp Fire
O50	Youth Development Programs, Other
O51	Youth Community Service Clubs
O52	Youth Development - Agricultural
O53	Youth Development - Business
O54	Youth Development - Citizenship Programs
O55	Youth Development - Religious Leadership
O99	Youth Development N.E.C.

Human Services - Multipurpose and Other

P01	Alliance/Advocacy Organizations
P02	Management & Technical Assistance
P03	Professional Societies, Associations
P05	Research Institutes and/or Public Policy Analysis
P11	Single Organization Support
P12	Fund Raising and/or Fund Distribution
P19	Nonmonetary Support N.E.C.
P20	Human Service Organizations - Multipurpose
P21	American Red Cross
P22	Urban League
P24	Salvation Army
P26	Volunteers of America
P27	Young Men's or Women's Associations (YMCA, YWCA, YWHA, YMHA)
P28	Neighborhood Centers, Settlement Houses
P29	Thrift Shops
P30	Children's, Youth Services
P31	Adoption
P32	Foster Care
P33	Child Day Care
P40	Family Services
P42	Single Parent Agencies, Services
P43	Family Violence Shelters, Services
P44	Homemaker, Home Health Aide
P45	Family Services, Adolescent Parents
P46	Family Counseling
P50	Personal Social Services
P51	Financial Counseling, Money Management
P52	Transportation, Free or Subsidized
P58	Gift Distribution
P60	Emergency Assistance (Food, Clothing, Cash)
P61	Travelers' Aid
P62	Victims' Services
P70	Residential, Custodial Care
P72	Half-Way House (Short-Term Residential Care)
P73	Group Home (Long Term)
P74	Hospice
P75	Senior Continuing Care Communities
P80	Services to Promote the Independence of Specific Populations
P81	Senior Centers, Services
P82	Developmentally Disabled Centers, Services
P84	Ethnic, Immigrant Centers, Services
P85	Homeless Persons Centers, Services
P86	Blind/Visually Impaired Centers, Services
P87	Deaf/Hearing Impaired Centers, Services
P99	Human Services - Multipurpose and Other N.E.C.

International, Foreign Affairs, and National Security

Q01	Alliance/Advocacy Organizations
Q02	Management & Technical Assistance
Q03	Professional Societies, Associations
Q05	Research Institutes and/or Public Policy Analysis
Q11	Single Organization Support
Q12	Fund Raising and/or Fund Distribution
Q19	Nonmonetary Support N.E.C.
Q20	Promotion of International Understanding
Q21	International Cultural Exchange
Q22	International Student Exchange and Aid
Q23	International Exchanges, N.E.C.
Q30	International Development, Relief Services
Q31	International Agricultural Development
Q32	International Economic Development
Q33	International Relief
Q40	International Peace and Security
Q41	Arms Control, Peace Organizations
Q42	United Nations Association
Q43	National Security, Domestic
Q70	International Human Rights
Q71	International Migration, Refugee Issues
Q99	International, Foreign Affairs, and National Security N.E.C.

Civil Rights, Social Action, Advocacy

R01	Alliance/Advocacy Organizations
R02	Management & Technical Assistance
R03	Professional Societies, Associations
R05	Research Institutes and/or Public Policy Analysis
R11	Single Organization Support
R12	Fund Raising and/or Fund Distribution
R19	Nonmonetary Support N.E.C.
R20	Civil Rights, Advocacy for Specific Groups
R22	Minority Rights
R23	Disabled Persons' Rights
R24	Women's Rights
R25	Seniors' Rights
R26	Lesbian, Gay Rights
R30	Intergroup, Race Relations
R40	Voter Education, Registration
R60	Civil Liberties Advocacy
R61	Reproductive Rights
R62	Right to Life
R63	Censorship, Freedom of Speech and Press Issues
R67	Right to Die, Euthanasia Issues
R99	Civil Rights, Social Action, Advocacy N.E.C.

Community Improvement, Capacity Building

S01	Alliance/Advocacy Organizations
S02	Management & Technical Assistance
S03	Professional Societies, Associations

S05	Research Institutes and/or Public Policy Analysis
S11	Single Organization Support
S12	Fund Raising and/or Fund Distribution
S19	Nonmonetary Support N.E.C.
S20	Community, Neighborhood Development, Improvement (General)
S21	Community Coalitions
S22	Neighborhood, Block Associations
S30	Economic Development
S31	Urban, Community Economic Development
S32	Rural Development
S40	Business and Industry
S41	Promotion of Business
S43	Management Services for Small Business, Entrepreneurs
S46	Boards of Trade
S47	Real Estate Organizations
S50	Nonprofit Management
S80	Community Service Clubs
S81	Women's Service Clubs
S82	Men's Service Clubs
S99	Community Improvement, Capacity Building N.E.C.

Philanthropy, Voluntarism, and Grantmaking Foundations

T01	Alliance/Advocacy Organizations
T02	Management & Technical Assistance
T03	Professional Societies, Associations
T05	Research Institutes and/or Public Policy Analysis
T11	Single Organization Support
T12	Fund Raising and/or Fund Distribution
T19	Nonmonetary Support N.E.C.
T20	Private Grantmaking Foundations
T21	Corporate Foundations
T22	Private Independent Foundations
T23	Private Operating Foundations
T30	Public Foundations
T31	Community Foundations
T40	Voluntarism Promotion
T50	Philanthropy, Charity, Voluntarism Promotion, General
T70	Fund Raising Organizations That Cross Categories
T90	Named Trusts/Foundations N.E.C.
T99	Philanthropy, Voluntarism, and Grantmaking Foundations N.E.C.

Science and Technology Research Institutes, Services

U01	Alliance/Advocacy Organizations
U02	Management & Technical Assistance
U03	Professional Societies, Associations
U05	Research Institutes and/or Public Policy Analysis
U11	Single Organization Support
U12	Fund Raising and/or Fund Distribution
U19	Nonmonetary Support N.E.C.
U20	Science, General
U21	Marine Science and Oceanography
U30	Physical Sciences, Earth Sciences Research and Promotion
U31	Astronomy
U33	Chemistry, Chemical Engineering
U34	Mathematics
U36	Geology
U40	Engineering and Technology Research, Services
U41	Computer Science
U42	Engineering
U50	Biological, Life Science Research
U99	Science and Technology Research Institutes, Services N.E.C.

Social Science Research Institutes, Services

V01	Alliance/Advocacy Organizations
V02	Management & Technical Assistance
V03	Professional Societies, Associations
V05	Research Institutes and/or Public Policy Analysis
V11	Single Organization Support
V12	Fund Raising and/or Fund Distribution
V19	Nonmonetary Support N.E.C.
V20	Social Science Institutes, Services
V21	Anthropology, Sociology
V22	Economics (as a social science)
V23	Behavioral Science
V24	Political Science
V25	Population Studies
V26	Law, International Law, Jurisprudence
V30	Interdisciplinary Research
V31	Black Studies
V32	Women's Studies
V33	Ethnic Studies
V34	Urban Studies
V35	International Studies
V36	Gerontology (as a social science)
V37	Labor Studies V99 Social Science Research Institutes, Services N.E.C.

Public, Society Benefit - Multipurpose and Other

W01	Alliance/Advocacy Organizations
W02	Management & Technical Assistance
W03	Professional Societies, Associations
W05	Research Institutes and/or Public Policy Analysis
W11	Single Organization Support
W12	Fund Raising and/or Fund Distribution
W19	Nonmonetary Support N.E.C.
W20	Government and Public Administration
W22	Public Finance, Taxation, Monetary Policy
W24	Citizen Participation
W30	Military, Veterans' Organizations
W40	Public Transportation Systems, Services
W50	Telephone, Telegraph and Telecommunication Services
W60	Financial Institutions, Services (Non-Government Related)
W61	Credit Unions
W70	Leadership Development
W80	Public Utilities
W90	Consumer Protection, Safety
W99	Public, Society Benefit - Multipurpose and Other N.E.C.

Religion Related, Spiritual Development

X01	Alliance/Advocacy Organizations
X02	Management & Technical Assistance
X03	Professional Societies, Associations
X05	Research Institutes and/or Public Policy Analysis
X11	Single Organization Support
X12	Fund Raising and/or Fund Distribution
X19	Nonmonetary Support N.E.C.
X20	Christian
X21	Protestant
X22	Roman Catholic
X30	Jewish
X40	Islamic
X50	Buddhist
X70	Hindu
X80	Religious Media, Communications Organizations
X81	Religious Film, Video
X82	Religious Television
X83	Religious Printing, Publishing
X84	Religious Radio
X90	Interfaith Issues
X99	Religion Related, Spiritual Development N.E.C.

Mutual/Membership Benefit Organizations, Other

Y01	Alliance/Advocacy Organizations
Y02	Management & Technical Assistance
Y03	Professional Societies, Associations
Y05	Research Institutes and/or Public Policy Analysis
Y11	Single Organization Support
Y12	Fund Raising and/or Fund Distribution
Y19	Nonmonetary Support N.E.C.
Y20	Insurance Providers, Services
Y22	Local Benevolent Life Insurance Associations, Mutual Irrigation and Telephone Companies, and Like Organizations
Y23	Mutual Insurance Company or Association
Y24	Supplemental Unemployment Compensation
Y25	State-Sponsored Worker's Compensation Reinsurance Organizations
Y30	Pension and Retirement Funds
Y33	Teachers Retirement Fund Association
Y34	Employee Funded Pension Trust
Y35	Multi-Employer Pension Plans
Y40	Fraternal Beneficiary Societies
Y42	Domestic Fraternal Societies
Y43	Voluntary Employees Beneficiary Associations (Non-Government)
Y44	Voluntary Employees Beneficiary Associations (Government)
Y50	Cemeteries, Burial Services
Y99	Mutual/Membership Benefit Organizations, Other N.E.C.

Unknown

Z99	Unknown

You must complete the Form 1023-EZ Eligibility Worksheet in the Instructions for Form 1023-EZ to determine if you are eligible to file this form. Form 1023-EZ is filed electronically **only** on Pay.gov. Go to www.irs.gov/form1023ez for additional filing information.

Form **1023-EZ**

(June 2014)

Department of the Treasury
Internal Revenue Service

Streamlined Application for Recognition of Exemption Under Section 501(c)(3) of the Internal Revenue Code

▶ **Do not enter social security numbers on this form as it may be made public.**

▶ **Information about Form 1023-EZ and its separate instructions is at *www.irs.gov/form1023*.**

OMB No. 1545-0056

Note: *If exempt status is approved, this application will be open for public inspection.*

☐ **Check this box to attest that you have completed the Form 1023-EZ Eligibility Worksheet in the current instructions, are eligible to apply for exemption using Form 1023-EZ, and have read and understand the requirements to be exempt under section 501(c)(3).**

Part I Identification of Applicant

1a Full Name of Organization

b Address (number, street, and room/suite). If a P.O. box, see instructions. | **c** City | **d** State | **e** Zip Code + 4

2 Employer Identification Number | **3** Month Tax Year Ends (MM) | **4** Person to Contact if More Information is Needed

5 Contact Telephone Number | **6** Fax Number (optional) | **7** User Fee Submitted

8 List the names, titles, and mailing addresses of your officers, directors, and/or trustees. (If you have more than five, see instructions.)

First Name:	Last Name:	Title:	
Street Address:	City:	State:	Zip Code + 4:
First Name:	Last Name:	Title:	
Street Address:	City:	State:	Zip Code + 4:
First Name:	Last Name:	Title:	
Street Address:	City:	State:	Zip Code + 4:
First Name:	Last Name:	Title:	
Street Address:	City:	State:	Zip Code + 4:
First Name:	Last Name:	Title:	
Street Address:	City:	State:	Zip Code + 4:

9 a Organization's Website (if available):

b Organization's Email (optional):

Part II Organizational Structure

1 To file this form, you must be a corporation, an unincorporated association, or a trust. **Check the box** for the type of organization.

☐ Corporation ☐ Unincorporated association ☐ Trust

2 ☐ **Check this box** to attest that you have the organizing document necessary for the organizational structure indicated above. (See the instructions for an explanation of **necessary organizing documents**.)

3 Date incorporated if a corporation, or formed if other than a corporation (MMDDYYYY): _____

4 State of incorporation or other formation: _____

5 Section 501(c)(3) requires that your organizing document must limit your purposes to one or more exempt purposes within section 501(c)(3).

☐ **Check this box** to attest that your organizing document contains this limitation.

6 Section 501(c)(3) requires that your organizing document must not expressly empower you to engage, otherwise than as an insubstantial part of your activities, in activities that in themselves are not in furtherance of one or more exempt purposes.

☐ **Check this box** to attest that your organizing document does not expressly empower you to engage, otherwise than as an insubstantial part of your activities, in activities that in themselves are not in furtherance of one or more exempt purposes.

7 Section 501(c)(3) requires that your organizing document must provide that upon dissolution, your remaining assets be used exclusively for section 501(c)(3) exempt purposes. Depending on your entity type and the state in which you are formed, this requirement may be satisfied by operation of state law.

☐ **Check this box** to attest that your organizing document contains the dissolution provision required under section 501(c)(3) or that you do not need an express dissolution provision in your organizing document because you rely on the operation of state law in the state in which you are formed for your dissolution provision.

Form 1023-EZ is filed electronically only on Pay.gov.

You must complete the Form 1023-EZ Eligibility Worksheet in the Instructions for Form 1023-EZ to determine if you are eligible to file this form. Form 1023-EZ is filed electronically **only** on Pay.gov. Go to www.irs.gov/form1023ez for additional filing information.

Part III Your Specific Activities

1 Enter the appropriate 3-character NTEE Code that best describes your activities (See the instructions): _____

2 To qualify for exemption as a section 501(c)(3) organization, you must be organized and operated exclusively to further one or more of the following purposes. By checking the box or boxes below, you attest that you are organized and operated exclusively to further the purposes indicated. **Check all that apply.**

- ☐ Charitable
- ☐ Religious
- ☐ Educational
- ☐ Scientific
- ☐ Literary
- ☐ Testing for public safety
- ☐ To foster national or international amateur sports competition
- ☐ Prevention of cruelty to children or animals

3 To qualify for exemption as a section 501(c)(3) organization, you must:

- Refrain from supporting or opposing candidates in political campaigns in any way.
- Ensure that your net earnings do not inure in whole or in part to the benefit of private shareholders or individuals (that is, board members, officers, key management employees, or other insiders).
- Not further non-exempt purposes (such as purposes that benefit private interests) more than insubstantially.
- Not be organized or operated for the primary purpose of conducting a trade or business that is not related to your exempt purpose(s).
- Not devote more than an insubstantial part of your activities attempting to influence legislation or, if you made a section 501(h) election, not normally make expenditures in excess of expenditure limitations outlined in section 501(h).
- Not provide commercial-type insurance as a substantial part of your activities.

☐ **Check this box** to attest that you have not conducted and will not conduct activities that violate these prohibitions and restrictions.

4 Do you or will you attempt to influence legislation? . . . . . ☐ **Yes** ☐ **No**
(If yes, consider filing Form 5768. See the instructions for more details.)

5 Do you or will you pay compensation to any of your officers, directors, or trustees? . . . . . ☐ **Yes** ☐ **No**
(Refer to the instructions for a definition of **compensation**.)

6 Do you or will you donate funds to or pay expenses for individual(s)? . . . . . ☐ **Yes** ☐ **No**

7 Do you or will you conduct activities or provide grants or other assistance to individual(s) or organization(s) outside the United States? . . . . . ☐ **Yes** ☐ **No**

8 Do you or will you engage in financial transactions (for example, loans, payments, rents, etc.) with any of your officers, directors, or trustees, or any entities they own or control? . . . . . ☐ **Yes** ☐ **No**

9 Do you or will you have unrelated business gross income of $1,000 or more during a tax year? . . . . . ☐ **Yes** ☐ **No**

10 Do you or will you operate bingo or other gaming activities? . . . . . ☐ **Yes** ☐ **No**

11 Do you or will you provide disaster relief? . . . . . ☐ **Yes** ☐ **No**

Part IV Foundation Classification

Part IV is designed to classify you as an organization that is either a private foundation or a public charity. Public charity status is a more favorable tax status than private foundation status.

1 If you qualify for public charity status, check the appropriate box (**1a – 1c** below) and skip to **Part V** below.

a ☐ **Check this box** to attest that you normally receive at least one-third of your support from public sources or you normally receive at least 10 percent of your support from public sources and you have other characteristics of a publicly supported organization. **Sections 509(a)(1) and 170(b)(1)(A)(vi)**.

b ☐ **Check this box** to attest that you normally receive more than one-third of your support from a combination of gifts, grants, contributions, membership fees, and gross receipts (from permitted sources) from activities related to your exempt functions and normally receive not more than one-third of your support from investment income and unrelated business taxable income. **Section 509(a)(2)**.

c ☐ **Check this box** to attest that you are operated for the benefit of a college or university that is owned or operated by a governmental unit. **Sections 509(a)(1) and 170(b)(1)(A)(iv)**.

2 If you are not described in items **1a – 1c** above, you are a private foundation. As a private foundation, you are required by section 508(e) to have specific provisions in your organizing document, unless you rely on the operation of state law in the state in which you were formed to meet these requirements. These specific provisions require that you operate to avoid liability for private foundation excise taxes under sections 4941-4945.

☐ **Check this box** to attest that your organizing document contains the provisions required by section 508(e) or that your organizing document does not need to include the provisions required by section 508(e) because you rely on the operation of state law in your particular state to meet the requirements of section 508(e). (See the instructions for explanation of the section 508(e) requirements.)

Form 1023-EZ is filed electronically only on Pay.gov.

You must complete the Form 1023-EZ Eligibility Worksheet in the Instructions for Form 1023-EZ to determine if you are eligible to file this form. Form 1023-EZ is filed electronically **only** on Pay.gov. Go to www.irs.gov/form1023ez for additional filing information.

Part V Reinstatement After Automatic Revocation

Complete this section only if you are applying for reinstatement of exemption after being automatically revoked for failure to file required annual returns or notices for three consecutive years, and you are applying for reinstatement under section 4 or 7 of Revenue Procedure 2014-11. (Check only one box.)

1 ☐ **Check this box** if you are seeking retroactive reinstatement under section 4 of Revenue Procedure 2014-11. By checking this box, you attest that you meet the specified requirements of section 4, that your failure to file was not intentional, and that you have put in place procedures to file required returns or notices in the future. (See the instructions for requirements.)

2 ☐ **Check this box** if you are seeking reinstatement under section 7 of Revenue Procedure 2014-11, effective the date you are filing this application.

Part VI Signature

☐ **I declare under the penalties of perjury that I am authorized to sign this application on behalf of the above organization and that I have examined this application, and to the best of my knowledge it is true, correct, and complete.**

PLEASE SIGN HERE

(Type name of signer) (Type title or authority of signer)

(Signature of Officer, Director, Trustee, or other authorized official) (Date)

Form 1023-EZ is filed electronically only on Pay.gov.

Printed on recycled paper