

**INFORMATION TECHNOLOGY  
(INTERMEDIARIES GUIDELINES) RULES, 2011  
AN ANALYSIS**



*sfllc.in*

*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

<b>ACMA</b>	Australian Communications and Media Authority
<b>Cr.PC</b>	Code of Criminal Procedure
<b>CRAC</b>	Cyber Regulation Advisory Committee
<b>DEITy</b>	Department of Electronics and Information Technology
<b>EU</b>	European Union
<b>IAMAI</b>	Internet and Mobile Association of India
<b>ISP</b>	Internet Service Provider
<b>IWF</b>	Internet Watch Foundation
<b>MCIT</b>	Ministry of Communications and Information Technology
<b>OSP</b>	Online Service Providers
<b>PUCL</b>	People's Union for Civil Liberties
<b>TRAI</b>	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.

According to the Indian Telecom Services Performance Indicators Report released by TRAI<sup>1</sup> 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

*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*

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<sup>2</sup>. 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

<sup>1</sup> Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators (October – December 2013)*, available at <http://www.trai.go.in/WriteReadData/PIRReport/Documents/Indicator%20Report's%20-%20Dec-2013.pdf> (last visited April 1, 2014)

<sup>2</sup> The full report is available at [http://www.iamai.in/rsh\\_pay.aspx?rid=rXiopaUzE7s=](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 cyberspace. 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](http://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 opposition, 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(CrI) 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<sup>3</sup> 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<sup>4</sup> **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.

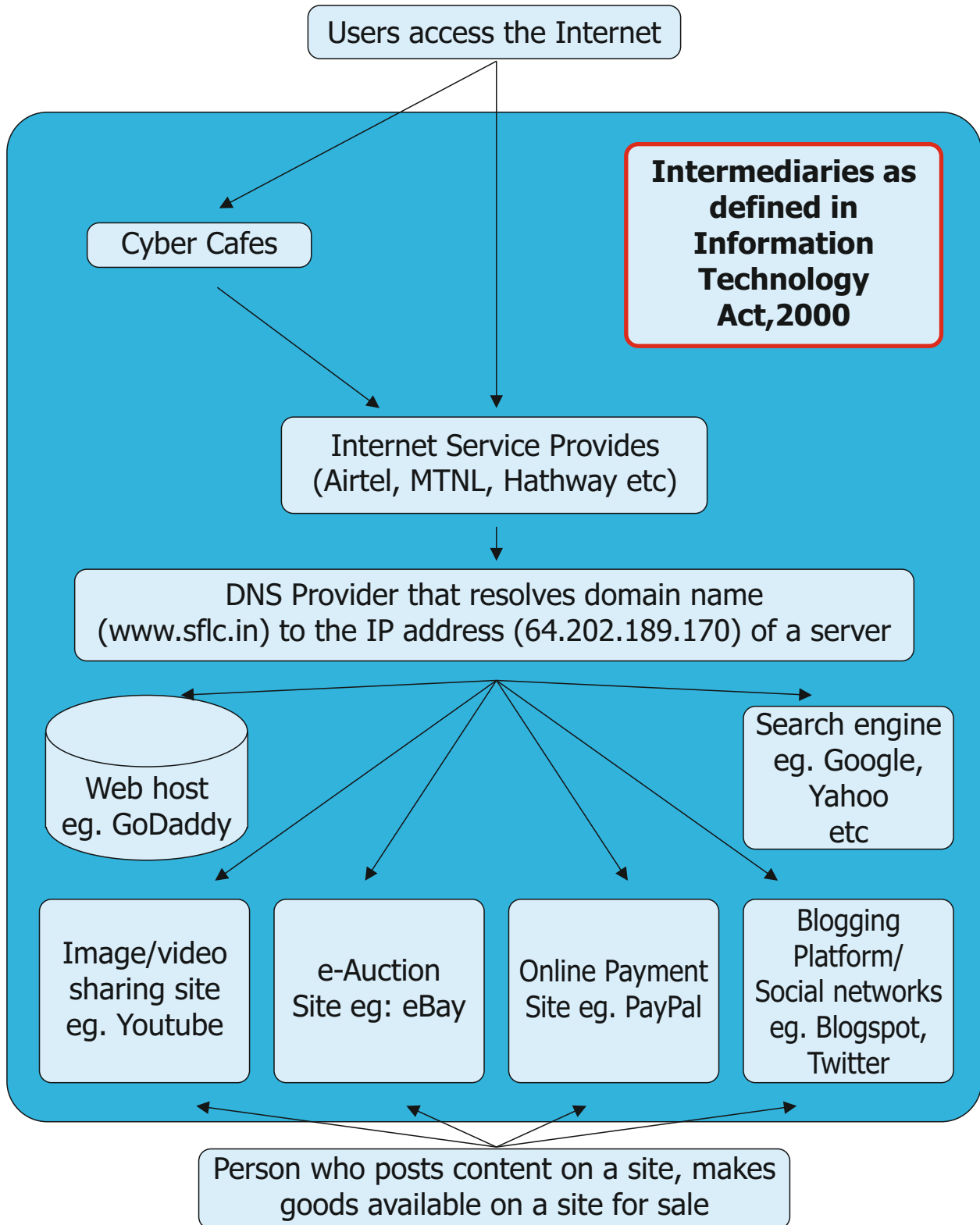
---

<sup>3</sup> 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](http://www.deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/ITAct.doc) (last visited on July 13, 2014)

<sup>4</sup> 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<sup>5</sup> 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.

<sup>5</sup> 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<sup>6</sup> 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)<sup>7</sup> of the Intermediaries Guidelines Rules lists the categories of information, if posted online, which could be considered as illegal. According to Rule 3(4)<sup>8</sup> 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.**

<sup>6</sup> Avnish Bajaj v. State, 150 (2008) DLT 769 and Aneeta Hada v. Godfather Travels and Tours Pvt. Ltd., AIR 2012 SC 2795

<sup>7</sup> 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 –*

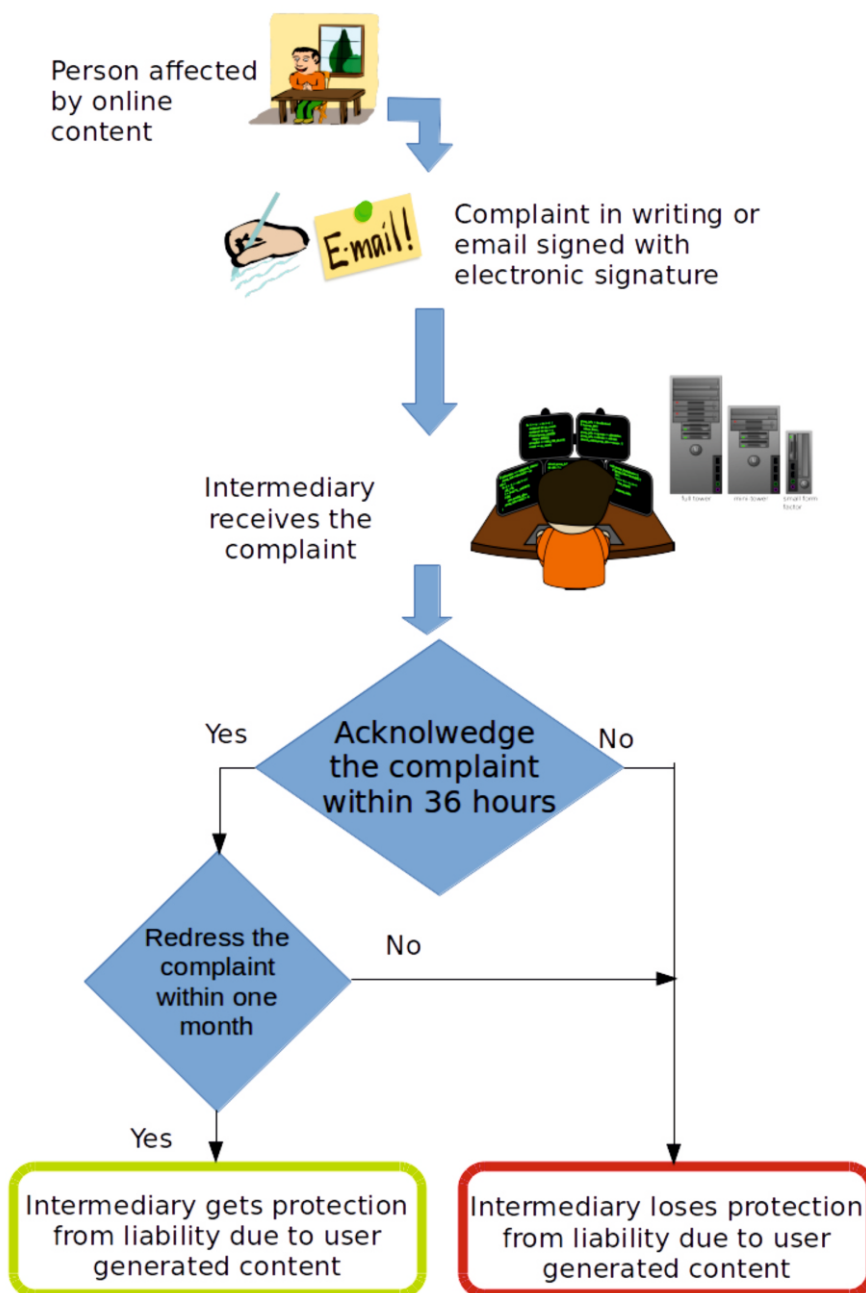
- (a) belongs to another person and to which the user does not have any right to;*
- (b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging 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;*

<sup>8</sup> 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<sup>9</sup> 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.



<sup>9</sup> 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](http://deity.gov.in/sites/upload_files/dit/files/Clarification%2079rules%281%29.pdf), (last visited April 1, 2014)

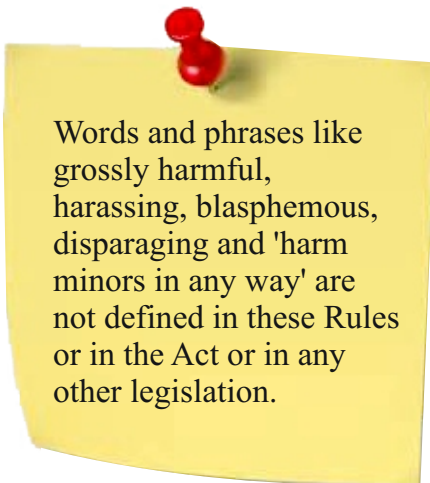


## 3.2 The Rules - Opinions of users and businesses

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.



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](http://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/cartoonsagainstcorruption-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<sup>10</sup> 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.

<sup>10</sup> 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

**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.**

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 thirty-six 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.*<sup>11</sup> 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.

### 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.

<sup>11</sup> 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.<sup>12</sup> 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.<sup>13</sup> 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 subsection (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

<sup>12</sup> Yahoo India Pvt. Ltd. V Union of India & Another, W.P.(C).No. 6654/2011

<sup>13</sup> 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<sup>14</sup> and the Communications Decency Act<sup>15</sup> 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,

<sup>14</sup> Digital Millennium Copyright Act, available at <http://www.copyright.gov/title17/92chap5.html#512> (last visited April 1, 2014)

<sup>15</sup> Copyright Act, available at <http://www.law.cornell.edu/uscode/text/47/230>. (last visited April 1, 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 (1) 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 An r. Vs. The Union of India (UOI) and Ors.*<sup>16</sup>, 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

*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.*

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

<sup>16</sup> 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.*<sup>17</sup>, 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*<sup>18</sup>, 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*<sup>19</sup>, the Hon'ble Supreme Court held that:

---

<sup>17</sup> (1997)1 SCC 301

<sup>18</sup> 1995 AIR SC 1236

<sup>19</sup> (1995) 5 SCC 139

“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.**

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*<sup>20</sup>, and *R. Raj Gopal v. State of Tamil Nadu*<sup>21</sup>. 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.*<sup>22</sup>, 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.

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*

<sup>20</sup> (1975) 2 SCC 148

<sup>21</sup> (1994) 6 SCC 632

<sup>22</sup> (1997) 1 SCC 301

*Liberties (PUCL) Vs. Union of India (UOI) and Anr.*<sup>23</sup> 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. Rule 3(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<sup>24</sup> which transposed the provisions in Directive 2000/31/EC<sup>25</sup> 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:

<sup>23</sup> Supra. 20

<sup>24</sup> Electronic Commerce Regulations, 2002, available at <http://www.legislation.gov.uk/cy/uksi/2002/2013/made>, (last visited July 13, 2014)

<sup>25</sup> Directive 2000/31/EC of the European Parliament, available at [http://eurlex.europa.eu/legalcontent/EN/ALL/;ELX\\_SESSIONID=52sgTOFGkhW0f3cPl3MSrDfmWKb1gzbg4DY7pyMvQvYySHFSmqz!](http://eurlex.europa.eu/legalcontent/EN/ALL/;ELX_SESSIONID=52sgTOFGkhW0f3cPl3MSrDfmWKb1gzbg4DY7pyMvQvYySHFSmqz!-735511499?uri=CELEX:32000L0031)

[-735511499?uri=CELEX:32000L0031](http://eurlex.europa.eu/legalcontent/EN/ALL/;ELX_SESSIONID=52sgTOFGkhW0f3cPl3MSrDfmWKb1gzbg4DY7pyMvQvYySHFSmqz!-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<sup>26</sup> and practices recommended by organizations that issue self regulatory code of practices. The Defamation (Operators of Websites) Regulations 2013<sup>27</sup> 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.

<sup>26</sup> Defamation Act, 2013, available at <http://www.legislation.gov.uk/ukpga/2013/26/contents/enacted>, (last visited July 13, 2014)

<sup>27</sup> 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<sup>28</sup> 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.*

<sup>28</sup> 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<sup>29</sup>, 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<sup>30</sup> 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<sup>31</sup> 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'**

<sup>29</sup> Supra. 13

<sup>30</sup> Section 32, Trademark Act, 1946, available at [http://www.uspto.gov/trademarks/law/Trademark\\_Statutes.pdf](http://www.uspto.gov/trademarks/law/Trademark_Statutes.pdf) (last visited July 13, 2014)

<sup>31</sup> Copyright Regulations, 1969, available at [http://www.austlii.edu.au/au/legis/cth/consol\\_reg/cr1969242/s20j.html](http://www.austlii.edu.au/au/legis/cth/consol_reg/cr1969242/s20j.html), (last visited July 13, 2014)

The Copyright Act 1968<sup>32</sup> provides safe harbour protection only to 'internet service providers'<sup>33</sup>. 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 categories 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 Internet. The Broadcasting Services Amendment (Online Services) Act 1999<sup>34</sup> (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<sup>35</sup>. This classification<sup>36</sup> 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

<sup>32</sup> Copyright Act, 1968, available at [http://www.austlii.edu.au/au/legis/cth/consol\\_act/ca1968133/](http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/) (last visited July 13, 2014)

<sup>33</sup> 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](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](http://www.austlii.edu.au/au/legis/cth/num_act/claa2004325/sch1.html) (last visited July 13, 2014)

<sup>34</sup> 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<sup>37</sup>, 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.

<sup>35</sup> 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)

<sup>36</sup> National Classification Code, May 2005, available at <http://www.comlaw.gov.au/Details/F2013C00006>, (last visited July 13, 2014)

<sup>37</sup> 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	<p><b>Copyright:</b>            Category A (Mere conduit)            Category B (Caching)            Category C (Hosting)            Category D (Location tool - links)</p> <p><b>Prohibited Content:</b>            Hosting service            Live content service            Links Service</p>	Yes	Yes	Yes
Brazil	<p><b>Internet connection providers</b>  <b>Internet application providers</b></p>	Yes	Yes	No
Canada	<p><b>Copyright:</b>            Communications service            Caching service            Hosting Service</p>	Yes	Yes	Yes
China	<p>Conduits            Caching service            Hosting service            Referral service</p>	Yes	Yes	Yes
France	<p>Mere conduits            Hosting service            Caching service</p>	Yes	No	No
Germany	<p>Mere access providers            Hosting providers            Caching providers</p>	Yes	No	No
India	N/A	Yes	Yes	No
Japan	N/A	Yes	Yes	Yes
New Zealand	<p><b>Copyright:</b>            Transmission service            Routing service            Connection service            Hosting service</p> <p><b>Other unlawful content:</b>            N/A</p>	Yes	Yes	No
Republic of Korea	N/A	Yes	Yes	Yes



South Africa	Mere conduit Caching service Hosting service Information location tools	Yes	Yes	No
UK	<b>Copyright:</b> Mere conduit Hosting service Caching service	Yes	Yes	Yes
	<b>Defamatory content:</b> N/A	Yes	Yes	Yes
USA	<b>Copyright:</b> 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 <i>subjudice</i> ; 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 <i>mandatory</i> as per the Rules, there is no precensorship; intermediaries are only required to <i>initiate</i> 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 <i>initiate</i> 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 40<sup>th</sup> 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 31<sup>st</sup> 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<sup>38</sup> 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 Rule 3(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.

<sup>38</sup> 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 Rajeev. 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)<sup>39</sup>.

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. Rajeev'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

<sup>39</sup> The video of the speech by Mr. Arun Jaitley is available at <http://www.youtube.com/watch?v=9La4zgCyiU>

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 compulsion 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 pre-censorship 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 pre-censorship 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. Rajeev'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. Rajeev'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<sup>40</sup> 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*

<sup>40</sup> 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](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<sup>41</sup> 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,

<sup>41</sup> 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 Economics, March 2014, available at [http://globalnetworkinitiative.org/sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics\\_March%202014\\_0.pdf](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 counterfeit 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 entrepreneurs 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<sup>42</sup> 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

<sup>42</sup> Article 19, *Internet Intermediaries: Dilemma of Liability*, available at [http://www.article19.org/data/files/Intermediaries\\_ENGLISH.pdf](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 (30<sup>th</sup> April 2013)
- Mumbai, Maharashtra (7<sup>th</sup> May 2013)
- Bangalore, Karnataka (10<sup>th</sup> May 2013)
- Cochin, Kerala (9<sup>th</sup> 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

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

*There should be classification on the basis of content, user and intermediary.*

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 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.

- 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.*<sup>43</sup> on telephone tapping and statutes.

<sup>43</sup>(1997)1 SCC 301

## 9. Conclusion

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.

**As technology evolves at a fast pace, the law should not be found wanting.**

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<sup>44</sup> 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.

<sup>44</sup> 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](http://www.sflc.in)**



This work is licensed under a Creative Commons  
Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) License.