Chinmayi Arun and Sarvjeet Singh

NOC ONLINE INTERMEDIARIES CASE STUDIES SERIES: ONLINE INTERMEDIARIES IN INDIA

February 18, 2015
National Law University, Delhi

WITHIN THE

GLOBAL NETWORK OF **INTERNET AND SOCIETY** RESEARCH CENTERS

NoC Online Intermediaries Case Studies Series: Online Intermediaries in India

Chinmayi Arun and Sarvjeet Singh
National Law University

Editorial Note: Context, Character, and Purpose of the Case Study

This case study is part of a globally coordinated, independent academic research project by the Global Network of Interdisciplinary Internet & Society Research Centers (NoC). Facilitated by the Berkman Center for Internet & Society at Harvard University, the project is the first output of a larger policy-oriented research initiative that examines the rapidly changing landscape of online intermediary governance at the intersection of law, technology, norms, and markets. In concert with other research projects, it seeks to develop criteria, comparative methods, and a shared data repository, and to compile insights and lessons learned across diverse communities of knowledge aimed at informing and improving Internet policy-making globally.

The initial research output consists of a case study series exploring online intermediary liability frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam, and a synthesis paper that seeks to distill key observations and provide a high-level analysis of some of the structural elements that characterize varying governance frameworks, with a focus on intermediary liability regimes and their evolution.

The authors of these case studies have participated in a multi-step process of in-person consultations and remote collaborations among a global team of researchers from the Network of Centers. Additionally, the case studies are based on a set of broader questions regarding the role of online intermediaries in the digital age.[1]

The research effort is grounded in a diversity of global perspectives and collaborative research techniques, committed to objective and independent academic standards, and aspires to be useful, actionable, and timely for policymakers and stakeholders. More broadly, the Network of Centers seeks to contribute to a more generalized vision and longer-term strategy regarding the role of academic research, facilitation and convening, and education and communication in the Internet age. For additional information on the initiative, please contact Urs Gasser, Berkman Center for Internet & Society, at ugasser@cyber.law.harvard.edu

[1] The process is documented at: "Online Intermediaries: Functions, Values, and Governance Options", The Global Network of Internet & Society Research Centers, 2014 https://drive.google.com/file/d/0B_ToTBKP5ITVWTl0UzV0U3B2RlU/view?usp=sharing.

Abstract: This case study maps and analyzes online intermediary liability in India. It begins with the landscape of online intermediaries in India, highlighting intermediaries of special interest. This includes, for instance, platforms used to arrange marriages, which are much more popular in India than dating platforms because of Indian social norms. The second section of the paper attempts to map in detail the governance mechanisms applicable to online intermediaries in India – this includes the licensing system used for internet service providers, the Information Technology Act, and the Copyright Act. The likelihood of generally applicable criminal law in India (such as the Indian Penal Code) as a potential source of intermediary liability is also discussed briefly. The final part of the paper assesses the impact of the governance framework, ties together its different themes of content blocking, interception of data, and notice and takedown of content. It analyzes the law under which these activities take place, from the perspective of good governance principles such as transparency and accountability. It also considers whether the governance framework for online intermediaries treats online speech in a manner that is consistent with the Indian constitution. The serious flaws in the systems followed in India are apparent through this assessment – the lack of transparency and accountability suggest that over-regulation of constitutionally protected speech is likely to result in very little protection of primary speakers' rights.

Table of Contents

I. Introduction 1
A. Top Websites in India 2
1. Search Engines 3
2. Social Media Websites: 3
B. Intermediaries of Interest in India 4
II. Governance Mechanisms and Legal Frameworks for Intermediary Liability in India . 6
A. Licensing System for Internet Service Providers 6
B. The Information Technology Act, 2000 8
1. Safe Harbor, 'Due Diligence,' and Editorial Control 10
2. Information Technology (Intermediaries Guidelines) Rules, 2011 12
3. Blocking Orders Under the IT Act 14
4. Interception Under the IT Act 16
C. The Copyright Act, 1957 18
III. Impact Assessment 21
A. Government-Ordered Blocking of Content 24
B. Notice and Takedown 26
C. Interception of Information by Intermediaries 28
IV. Cases currently before the Supreme Court 30
A. Rajeev Chandrasekhar 30
1. Information Technology (Intermediaries Guidelines) Rules, 2011 30
B. Common Cause 30
1. Section 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 30
C. Moutshut.com 31
D. Peoples' Union for Civil Liberties 31
1. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 31
2. Information Technology (Intermediaries guidelines) Rules, 2011 31
E. Internet and Mobile Association of India 32
1. Information Technology (Intermediaries guidelines) Rules, 2011 32
F. Kamlesh Vaswani 33
G. Sabu Mathew George 33

I. Introduction

The intermediary eco-system in India is still evolving. At a glance, it is apparent that the major online intermediaries in India are familiar global names. This is not surprising given the demographic that is currently accessing the Internet in India: digital access is concentrated in urban areas, and among literate people who are familiar with the languages used by international online platforms.

This paper begins with an attempt to outline the significant online intermediaries operating in India and the market share held by each. It also highlights some interesting online intermediaries, like CGNet Swara, that are significant for reasons other than market share. CGNet Swara is a hybrid platform catering to parts of rural India, allowing tribal people to create news reports using a simple voice mobile phone connection. Indian social norms also generate their own versions of global online platforms. While dating websites are ubiquitous globally, their Indian counterparts focus on 'arranging' marriages using criteria like caste, religion and skin-color, which are significant factors in what is referred to popularly as the 'marriage market'.

The second part of the paper discusses the regulatory framework that governs intermediary liability in India. It outlines very briefly the constitutional framework within which intermediaries operate. It then proceeds to offer an indication of the criminal and civil liability that might apply to intermediaries without safe harbor protection. This safe harbor protection comes from the Information Technology Act, which offers conditional immunity to intermediaries. This immunity and the conditions attached to it – including intermediaries' obligations in the context of content blocking, interception of information, and notice and takedown – are discussed in some detail in this part. Also discussed is the Copyright Act's different safe harbor framework and the ex parte court copyright-infringement related orders that are increasingly prevalent in India.

The third part of this paper builds on the facts set out in the second part by offering an analysis, supported with data wherever possible, of the impact that the regulatory framework has on online intermediaries and the content that they are willing to host. This part of the paper considers the transparency and accessibility of the legal rules, in order to assess whether intermediaries are easily able to understand what they need to do to comply. It examines the framework's incentives to see whether a chilling effect is created. It also considers the transparency and accountability of government ordered blocking and interception to evaluate whether this liability regime offers any safeguards from censorship or surveillance by proxy.

The notice and takedown process set up under the Information Technology Act (IT Act) and the Copyright Act are controversial especially in terms of the chilling effect that they have on speech. Also of concern are several petitions currently before the Supreme Court of India. While some of these petitions seek to strike down the notice and takedown regime set up by the IT Act on grounds that it violates constitutional rights, others seek to reinstate a strict liability regime for obscene content online. The Supreme Court's ruling in these cases will shape the future of intermediary liability law in India. They are introduced at the end of this piece.

India currently has the world's third largest Internet consumer base after China and the United States,[2] with a total of 238.71 million subscribers as of December 2013[3] and 205 million users as of October 2013.[4] However, the number of active Internet users (i.e. users accessing the Internet at least once a month) was a much lower 149 million as of June 2013.[5] The users' engagement with the online space is also low, with Internet users in India spending only 20 to 25 hours on average online per month.[6]

A. Top Websites in India

The top websites in India, according to commercial web traffic data collected by Alexa, an analytical website, are as follows:[7]

S. No.	Top Websites in India
1.	google.co.in
2.	google.com
3.	facebook.com
4.	youtube.com
5.	yahoo.com
6.	wikipedia.org
7.	blogspot.in
8.	flipkart.com
9.	indiatimes.com
10.	linkedin.com
11.	twitter.com
12.	jabong.com

[2]Moulishree Srivastava, *Internet base in India crosses 200 million mark*, MINT (Nov. 13, 2013), http://www.livemint.com/Consumer/9pWsphmYL2YjdisfO7bGLM/Internet-base-in-India-crosses-200-million-mark.html.s

[3]Telecom Regulatory Authority of India, The Indian Telecom Services Performance Indicators: April - June, 2013, xii, 27 (Dec. 2013), *available at* http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator%20Reports%20-%20Jun-02122013.pdf.

[4]*Internet Users in India Crosses 200 Million Mark*, IAMAI (Nov. 13, 2013), http://www.iamai.in/PRelease_detail.aspx?nid=3222&NMonth=11&NYear=2013.

[5]*IAMAI Internet in India 2013*, Internet and Mobile Association of India, 2 (2013).

[6] Chandra Gnanasambandam and Anu Madgavkar, *Online and upcoming: The Internet's impact on India*, MCKINSEY & COMPANY (Dec. 2012), *available at* http://www.mckinsey.com/insights/high_tech_telecoms_Internet/indias_Internet_opportunity.

[7]*Top sites in India*, ALEXA (July 24, 2014), *available at* http://www.alexa.com/topsites/countries/IN.

13.	amazon.com
14.	stackoverflow.com
15.	wordpress.com

Figure 1. *Top Websites in India*

This data indicates that thirteen of the top fifteen websites are based outside India. The two exceptions are flipkart.com (an online retailer that reaches markets similar to those targeted by Amazon) and indiatimes.com (a content portal owned by Indian media company Bennett, Coleman and Co. Ltd.).

1. Search Engines

S. No.	Name of Search Engine	Market Share (%)[8]
1.	Google	97.03
2.	Yahoo!	1.12
3.	Bing	0.77

Figure 2*. Search Engines (Data from StatCounter)*

2. Social Media Websites:

S. No.	Name of Social Media Site[9]	Market Share (%)[10]
1.	Facebook	81.16
2.	YouTube	5.68
3.	Twitter	4.77
4.	StumbleUpon	2.36
5.	Tumblr	1.84
6.	Pinterest	1.51
7.	NowPublic	0.78
8.	LinkedIn	0.71

[8] *Top 5 Search Engines in India from June 2013 to June* 2014, *available at* http://gs.statcounter.com/#all-search_engine-IN-monthly-201306-201406.

[9] The data combines Micro blogs, Social media; User generated content platforms types of intermediaries as provided in the guiding questions document.

[10] *Top 7 Social Media sites in India from June 2013 to June* 2014, *available at* http://gs.statcounter.com/#all-social_media-IN-monthly-201306-201406.

9.	Google+	0.63
10.	Reddit	0.46

Figure 3. *Social Media Websites (Data from StatCounter)*

Facebook has the largest user base in India with 93 million users, followed by Twitter with its estimated 33 million accounts,[11] and LinkedIn, which has 24 million users.[12] According to the Comscore India Digital Future in Focus Report 2013, Facebook is the most popular social media site in India, capturing the maximum screen time with access to 86% of the user base in India and 59,642,000 unique visitors in 2012-2013.[13] The report suggests that Facebook is followed by LinkedIn, which is the next most popular, with 11,127,000 visitors, followed by Twitter, which had 3,884,000 unique visitors.[14] An IAMAI report suggests that 96% of the total number of social media users use Facebook, while 57% use Google plus, and 49% use Orkut.[15] The video-sharing platform YouTube has over 55 million unique users a month in India,[16] and is used by 58% of 137 million Internet users in the country.[17]

B. Intermediaries of Interest in India

There are many intermediaries in India that were created in response to Indian social norms and markets. These include online matrimonial portals, which resemble online dating services in some ways, but have other design choices and actual functions that cater to Indian social norms. The first of these matrimonial portals began operation in 1996 and was called sagaai.com (subsequently shaadi.com),[18] owned by People Group. The online matrimony market is currently valued at around $83,000,000[19] and is expected to touch $250,000,000 by 2017.[20] In deference to widespread Indian practices about marrying within particular sub-groups, these portals enable

[11] Atish Patel, India's social media election battle, BBC NEWS INDIA (Mar. 31, 2014), http://www.bbc.com/news/world-asia-india-26762391.

[12] *LinkedIn India user base crosses 24 million; 277 million members worldwide*, NDTV (Feb. 12, 2014), http://gadgets.ndtv.com/social-networking/news/linkedin-india-user-base-crosses-24-million-277-million-members-worldwide-482512.

[13] *India Digital Future in 2013*, COMSCORE, 24 (Aug. 22 2013), *available at* http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_India_Digital_Future_in_Focus.

[14] *India Digital Future in 2013*, COMSCORE, 24 (Aug. 22 2013), *available at* http://www.comscore.com/Insights/Presentations_and_Whitepapers/2013/2013_India_Digital_Future_in_Focus.

[15] *Social Media in India – 2013*, INTERNET AND MOBILE ASSOCIATION OF INDIA, 6 (Oct. 2013).

[16] N Madhavan and Vivek Sinha, *We have 10,000 full-length Indian movies on YouTube: Google India chief*, HINDUSTAN TIMES (Sept. 17, 2013), http://www.hindustantimes.com/business-news/we-have-10-000-full-length-indian-movies-on-youtube-google-india-chief/article1 1123030.aspx.

[17] Rohin Dharmakumar, *Is Google Gobbling Up the Indian Internet Space?*, FORBES INDIA (Jul. 22, 2013), http://forbesindia.com/article/real-issue/is-google-gobbling-up-the-indian-Internet-space/35641/0#ixzz38Kf8IuNP.

[18] Satrajit Sen, *Arranged marriages over the Internet were a laughable idea when Shaadi.com started*, INDIA DIGITAL REVIEW (Dec. 5, 2011), http://www.indiadigitalreview.com/interviews/arranged-marriages-over-Internet-were-laughable-idea-when-shaadicom-started-anupam-g-mitt.

[19] Harsimran Julka & Apurva Vishwanath, *Matrimony portals making serious efforts to counter rising tide of divorces, ensure lasting unions*, ECONOMIC TIMES (June 26, 2013), http://articles.economictimes.indiatimes.com/2013-06-26/news/40206906_1_portals-online-bharatmatrimony-com.

[20] *Online marriage business may touch Rs.1,500 crore by 2017: Assocham*, INDIA TODAY (Dec. 18, 2013), http://indiatoday.intoday.in/story/online-marriage-business-may-touch-rs-1500-crore-by-2017-assocham/1/331691.html.

users to search for matches based on religion, caste, mother tongue, horoscope, skin tone, vegetarianism, alcohol consumption, and smoking habits. They enable parents to set up profiles for their offspring, allowing for the fact that many families 'arrange' marriages for young people and see the choice of partner as a family decision rather than an individual one. The consequence of this can be a violation of privacy and professional embarrassment for people who find that a wedding profile has been created for them without their consent. However, it is difficult to find lawsuits or complaints about these incidents since they take place between close family members and are usually handled informally. A more serious and fairly common problem in the context of matrimonial websites is fraud. News reports suggest that there are multiple cases of women and their families being duped by men who use these platforms to extort money by misrepresentation or blackmail.[21] The Government has issued a press release reminding these intermediaries of their obligation to disable harmful and unlawful information when it is reported, and to appoint Grievance Officers to assist with this process.[22] The press release also mentions the Indian Computer Emergency Response team works with social networking websites to disable fake accounts, and that this is more easily achieved for social networking websites with offices in India.[23]

In non-urban India, new platforms are being set up to bridge the digital divide even though broadband connectivity is still not available in these regions.[24] These platforms include initiatives like CGNet Swara, Kanoon Swara, and Graam Vani. CGNet Swara allows people in rural areas of central India with majorities of tribal populations to submit and listen to audio news reports regarding the area. The initiative receives an average of 200 calls per day and is driving the emergence of online reports on local issues.[25] The Gram Vaani[26] operates a Mobile Vaani initiative that connects reports from mobile phone users to stakeholders including governments and NGOs using an interactive voice response system. In the state of Jharkhand, it has over 100,000 users that call 2000 times a day.[27]

---

[21] Sadaf Aman, Frauds and Cheats Rule Matrimonial Sites, New Indian Express, http://www.newindianexpress.com/cities/hyderabad/2014/11/24/Fraud-and-Cheats-Rule-Matrimonial-Sites/article2537595.ece, last visited on 8th January 2015.

[22] *Steps to Prevent Frauds by Social Networking Sites and Matrimonial Sites*, PRESS INFORMATION BUREAU (21 Feb., 2014) http://pib.nic.in/newsite/PrintRelease.aspx?relid=104142.

[23] *Steps to Prevent Frauds by Social Networking Sites and Matrimonial Sites*, PRESS INFORMATION BUREAU (21 Feb., 2014) http://pib.nic.in/newsite/PrintRelease.aspx?relid=104142.

[24] As of 2013 only 60 million of the 190 million total Internet users were from rural India: *IAMAI Internet in India 2013*, Internet and Mobile Association of India, 2 (2013); The teledensity in rural areas is approximately 43 percent as compared to 140 percent teledensity in urban areas: TRAI, *Highlights on Telecom Subscription Data as on 30th April, 2014*, Press Release No. 35/2014 (June 26, 2014), http://www.trai.gov.in/WriteReadData/PressRealease/Document/PR-TSD-Apr,14.pdf.

[25] *India: Use Mobile Technology to Bring News to Isolated Tribal Communities*, International Centre for Journalists, http://www.icfj.org/knight-international-journalism-fellowships/fellowships/india-using-mobile-technology-bring-news-is-0.

[26] *Graam Vaani: About Us*, http://www.gramvaani.org/?page_id=76.

[27] *How Mobile Vaani Works*", http://www.gramvaani.org/?page_id=15.

Online recruitment websites such as 'naukri.com' and 'monster.com' have also gained immense popularity in India.[28]

II. Governance Mechanisms and Legal Frameworks for Intermediary Liability in India

Online intermediaries are subject to a fairly complex regulatory framework in India, which leaves them open to civil and criminal liability. The most significant laws governing intermediaries may be found in the Information Technology Act, 2000, and the Copyright Act, 1957. However there are circumstances in which more generally applicable legislation, such as the Indian Penal Code (1860), the Scheduled Caste and Scheduled Tribe (Prevention of Atrocities) Act (1989), the Protection of Children from Sexual Offences Act (2012), as well as the law of torts, may apply. If an online intermediary is not eligible for immunity from liability offered by the IT Act,[29] it could incur civil or criminal penalties for offences such as defamation,[30] obscenity,[31] sedition,[32] and/or copyright claims.[33]

The regulatory approach thus far is largely command and control, as is typical of the Indian legal system. However, this seems to be changing gradually as the architectural constraints of the Internet become more apparent. Online intermediaries, unlike Internet service providers (ISPs), cannot be subject to the domestic licensing regime, given that several of them do not have offices in India and are therefore out of the physical jurisdiction within which the Indian Government is easily able to implement its laws. Therefore, although ISPs are subject to several obligations through their licenses (discussed below in 2.1), international online intermediaries remain free of these constraints.

A. Licensing System for Internet Service Providers

Internet service providers are required to get licenses in India, and are subject to several obligations through their license terms. Content intermediaries, however, do not have to get licenses for operation, and one of the reasons for this might be that it would be very difficult to enforce such a requirement on intermediaries located in other jurisdictions. Of the various types of Internet intermediaries, it is telecommunication service providers, network service providers, and Internet service providers that require a license to offer services in India.

The regulatory framework for intermediaries originates in the Indian Telegraph Act,[34] which empowers the Central Government to issue licenses to establish, maintain, or work a telegraph.[35] The Department of Telecommunication acts as a licensor on behalf of the Central Government,

---

[28] Rebirth of e-Commerce in India, Ernst and Young (2013), *available at* http://www.ey.com/Publication/vwLUAssets/Rebirth_of_e-Commerce_in_India/$FILE/EY_RE-BIRTH_OF_ECOMMERCE.pdf.

[29] The Information Technology Act, 2000, § 79 (prior to the Information Technology Amendment Act, 2008).

[30] The Indian Penal Code, 1860, § 499; *Khushwant Singh and Anr.* v. *Maneka Gandhi*, A.I.R. 2002 Delhi 58 (India); Ratanlal and Dhirajlal, The Law of Torts 279 (26th ed. 2013).

[31] The Indian Penal Code, 1860, § 292, The Information Technology Act, 2000, § 67.

[32] The Indian Penal Code, 1860, § 124A.

[33] The Copyright Act, 1957, § 51.

[34] The Indian Telegraph Act, 1885, § 4

[35] The Indian Telegraph Act, 1885, § 3 (1AA)

and enters into agreements with companies for the provision of telecommunications and Internet Services.

There are three types of licenses for communication providers in India:

- The License Agreement for Provision of Internet Services ('ISP License')[36]
- The License Agreement For Provision Of Unified Access Services after Migration from CMTS ('UAS License')[37]
- The License Agreement for Unified License ('Unified License')[38]

The Government has taken to issuing only Unified Licenses since 2012. This might be an effort to consolidate and simplify the licensing process, since the Unified License covers various telecom services such as access, Internet, and long distance within a single license.[39] It contains a separate chapter for Internet services.

The licenses obligate licensee-intermediaries to block Internet sites, Uniform Resource Locators (URLs), Uniform Resource Identifiers (URIs), and/or individual subscribers, as identified and directed by the government in the interest of national security or public interest from time to time.[40] The licenses also declare that carriage of objectionable, obscene, unauthorized, or any other content, messages, or communications infringing copyright and intellectual property rights etc., in any form, is not permitted, and obligates licensees to prevent such carriage when specific instances are reported.[41]

The license agreements contain a number of provisions concerning data retention, disclosure, and the provision of services to enable surveillance.[42] They require ISPs to put in place systems that enable lawful monitoring and interception of communications by the Indian Government.[43] ISPs are also required to trace or monitor content such as communications that are obnoxious, malicious, or a nuisance,[44] and 'objectionable' communications.[45]

---

[36] Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.
[37]Licence Agreement for Provision of Unified Access Services after Migration from CMTS , http://www.auspi.in/policies/UASL.pdf.
[38]License Agreement for Unified License , http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.
[39] Department of Telecommunications, *Unified License*, http://www.dot.gov.in/licensing/unified-license
[40] Chapter IX clause 7.12, License Agreement for Unified License, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf clause 7.12, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.
[41] Chapter V clause 38.1, License Agreement for Unified License, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf clause 33.6, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.
[42] Chinmayi Arun and Ujwala Uppaluri, *Research Memorandum Concerning The Indian Surveillance Framework for iProbono* (2014).
[43] Chapter IX clause 8.1.1, License Agreement for Unified License, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf.
[44]Clause 33.4, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.
[45] Clause 33.6, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.; Chinmayi Arun and Ujwala Uppaluri, *Research Memorandum Concerning The Indian Surveillance Framework for iProbono* (2014).

At every international gateway or node having an outbound capacity of more than 2 MB/s, ISPs are required to set up monitoring centers equipped with appropriate monitoring systems in accordance with government specifications,[46] office space,[47] telephone lines,[48] and be accessible to monitoring agencies at all times.[49] ISPs must also facilitate Government access to various equipment, leased lines, record files, and logbooks of the ISPs.[50] Additionally, periodic inspections of Internet leased line customers at their premise are to be performed by the ISP within 15 days of commissioning an Internet line to check for possible misuse.[51]

The UAS & Unified Licenses require licensee service providers to provide the 'necessary facilities' to the Government to "counteract espionage, subversive acts, sabotage, or any other unlawful activity."[52] All three licenses obligate licensees to 'facilitate' the application of Section 5 of the Indian Telegraph Act, which deals with interception of communication.[53]

B. The Information Technology Act, 2000

The Information Technology Act, 2000 (referred to as 'IT Act') came into force on October 17th, 2010 and was meant to provide legal recognition of *electronic commerce.*[54] It was also meant to give effect to a UN General Assembly resolution on Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.[55] The IT Act was amended in 2008[56] in a manner that expanded the safe harbor protection significantly, thereby changing the intermediary liability regime substantially. The amendment emerged after the Report of the Expert Committee on the Proposed Amendments to the IT Act, 2000 suggested certain reforms, which would also ensure that the law relating to intermediary liability had more clarity and was closer to the framework in the EU E-Commerce Directive 2000/31/EC,[57] which was used to guide the revision of the IT Act.[58]

---

[46] Clause 34.27(a)(i), Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf. 34.27(a)(i)

[47] Clause 34.27(a)(ii), Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.

[48] Clause 34.27(a)(iii), Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.

[49] Clause 34.27, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf

[50] Clause 30.1, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.

[51] Clause 34.17, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf.

[52] Clause 41.1, Licence Agreement for Provision of Unified Access Services after Migration from CMTS , http://www.auspi.in/policies/UASL.pdf

[53] Clause 40.1, License Agreement for Unified License, http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf; clause 35.1, Licence Agreement for Provision of Internet Services, http://cca.ap.nic.in/i_agreement.pdf; clause 42.1 Licence Agreement for Provision of Unified Access Services after Migration from CMTS , http://www.auspi.in/policies/UASL.pdf.

[54] The Information Technology Act, 2000, preamble (prior to the Information Technology Amendment Act, 2008).

[55] G.A. Res. 51/162, Model Law on Electronic Commerce, U.N. Doc. A/RES/51/162 (Jan. 30, 1997).

[56] The Information Technology (Amendment) Act, 2008.

[57] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (June 8, 2000), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML.

[58] Department of Information Technology, Ministry of Communications & Information Technology, Government of India, Report of the Expert Committee on Proposed Amendments to Information Technology Act 2000, 46 (Aug. 2005), *available at* http://www.prsindia.org/uploads/media/Information%20Technology%20/bill93_2008122693_Report_of_Expert_Committee.pdf; Department of Information Technology, Ministry of Communications & Information TECHNOLOGY,

The IT Act, prior to amendment, protected intermediaries from liability[59] in a very limited manner. The immunity extended to a narrow set of intermediaries: it was provided only to a 'network service provider' which was defined as an intermediary, which in turn was defined as "any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.''[60] Additionally, protection was offered only with respect to offences committed under the IT Act, leaving intermediaries open to liability under other legislation for content that they hosted.

One of the concerns raised was that offering only 'network service providers' protection from liability might leave out a range of online intermediaries,[61] including the ones that provide online credit validation services.[62] It has also been argued that 'messages' were the only kind of content to which the safe harbor liability protection applied, and depending on how the term 'message' is interpreted, this may have narrowed the scope of the protection offered.[63] However, these concerns do not apply anymore, since the IT Act has been amended to expand both the immunity and the definition of the intermediaries that may claim this immunity.

Intermediaries with respect to electronic records are defined under the amended Section 2(w) of the Information Technology Act as "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-marketplaces, and cyber cafes."[64]

This was hailed by some commentators for its wider and clearer definition of intermediaries, which unambiguously included online intermediaries within its purview.[65] Others have pointed out that that although this new definition expands the number of entities that can claim safe harbor protection under the IT Act, it fails to make allowances for the functional differences between the different kinds of intermediaries.[66]

Section 2(w) includes a variety of very different intermediaries, such as telecom service providers, network service providers, Internet service providers, web-hosting service providers,

---

Government of India, Summary of the Report of the Expert Committee on Proposed Amendments to Information Technology Act 2000, ¶ 17 (Aug. 2005), *available at* http://deity.gov.in/content/report-expert-committee-amendments-it-act-2000-3.

[59]The Information Technology Act, 2000, § 79 (prior to the Information Technology Amendment Act, 2008).

[60]The Information Technology Act, 2000, § 2, cl. w (prior to the Information Technology Amendment Act, 2008).

[61]Apar Gupta, Commentary on Information Technology Act 295 (2nd ed. 2011); Thilini Kahandawaarachchi, *Liability of Internet Service Providers for Third Party Online Copyright Infringement: A Study of US and Indian laws*, 12 J. I.P.R. 553, 559 (2007); Priyambada Mishra and Angsuman Dutta, *Striking a Balance between Liability of Internet Service Providers and Protection of Copyright over the Internet: A Need of the Hour*, 14 J. I.P.R. 321, 324 (2009); Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120 (Dec. 2013); *See generally* Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 37 (2010).

[62]Apar Gupta, Commentary on Information Technology Act 295 (2nd ed. 2011).

[63]Apar Gupta, Commentary on Information Technology Act 295 (2nd ed. 2011).

[64] The Information Technology Act, 2000, § 2, cl. w.

[65]Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 37 (2010).

[66]Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).

search engines, online payment sites, online-auction sites, online-marketplaces or cyber cafes, in its scope. The obligations under the IT Act are such that all these intermediaries, online or offline, are subject to exactly the same legal regime.

Differential obligations may apply to different kinds of intermediaries owing to regulations that may be specific to their particular function, such as licenses for ISPs or banking regulations for financial intermediaries. However, the safe harbor protection for intermediaries includes immunity from liability under other legislations, and therefore intermediaries that meet the conditions for immunity in section 79 of the IT Act all get immunity and find themselves in a similar position regardless of their specific role or nature. It has been argued that by not taking into account the functional differences of the intermediaries, the efficacy of the immunity may be compromised.[67]

1. Safe Harbor, 'Due Diligence,' and Editorial Control

The amended safe harbor provision under Section 79 allows a wide spectrum of intermediaries to seek safe harbor protection from liability for any third party information, data, or communication link hosted by the third party. Section 79 ensures that the intermediaries' immunity from liability prevails over all other laws in force,[68] except for the Copyright Act and the Patents' Act.[69]

To be granted immunity under section 79, the intermediary must:

- Merely provide access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted;[70] or not initiate the transmission, select its receiver, or select or modify the information contained in the transmission;[71] and
- Observe due diligence[72] as provided by rules promulgated by the government in 2011.[73]

The use of the word "or" between the first two conditions stated above means that they are disjunctive in nature and only one needs to be satisfied in order for the intermediary to be granted immunity, along with fulfilling the third condition.[74]

Some commentators suggest that section 79 uses both the "mere conduit" and the "caching" principles, borrowed from the EU E-commerce Directive,[75] whereas others point out that the

[67]Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).
[68]The Information Technology Act, 2000, § 79, cl. 1.
[69]The Information Technology Act, 2000, § 81.
[70]The Information Technology Act, 2000, § 79, cl. 2(a).
[71]The Information Technology Act, 2000, § 79, cl. 2(b).
[72]The Information Technology Act, 2000, § 79, cl. 2(c).
[73]The Information Technology (Intermediaries guidelines) Rules, 2011.
[74] *Super Cassettes Industries Ltd* v. *MyspaceInc,* M.I.P.R. 2011 (2) 303 (India).
[75] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (June 8, 2000), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML; Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 121-22 (Dec. 2013).

language explicitly only discusses the mere conduit principle.[76] What is clear upon examination of section 79 is that to be eligible for immunity, the intermediary has to confine itself to transmission of information and not initiate transmission, select the receiver, or modify the information.[77] Services that would clearly be covered here because of their conduit function include telecommunications carriers, ISPs, and other backbone services.[78] However, caching services should also be included since they do fall within the definition of an intermediary under the amended IT Act (which includes those who store and host information),[79] and the immunity under section 79 seems to extend to all intermediaries with no specific exclusion of caching services. There is no reason why service providers who offer hosting services and do not fall afoul of the preconditions to the safe harbor protection should not qualify for immunity under section 79.

Wielding editorial control would almost certainly cause an intermediary to be excluded from the safe harbor protection. For one thing, it would amount to selection of information, such that the intermediary will fail one of the pre-requisites listed in Section 79(2).[80]

Controversially, the immunity from liability granted by section 79 is contingent upon intermediaries observing 'due diligence'.[81] This standard has been outlined in multiple cases, and the obligations that it entails are listed in detail in the Information Technology (Intermediaries

---

[76]Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, CENTRE FOR INTERNET & SOCIETY 20-23 (Apr. 10, 2012), *available at* http://cis-india.org/Internet-governance/intermediary-liability-in-india.

[77]*See also* Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 122 (Dec. 2013).

[78]Rajendra Kumar and Latha R. Nair, *Information Technology Act, 2000 and the Copyright Act, 1957: Searching for the Safest Harbor?*, 5 NUJS L. REV. 554, 562 (2012).

[79]S. 79. Exemption from liability of intermediary in certain cases.—(1)Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-section (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.

[80]Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 38 (2010).

[81]The Information Technology Act, 2000, § 79, cl. 2(c).

guidelines) Rules, 2011. The implications of this standard are discussed in more detail in the section on Intermediaries Guidelines below.

However, there are other ways in which even intermediaries that perform purely conduit or hosting services might find themselves liable, despite section 79. Section 79(3) limits the immunity offered by section 79, by outlining the circumstances under which an intermediary will be forbidden from claiming immunity:

- If the intermediary has conspired or abetted in the commission of the unlawful act.[82] This means that if the intermediary is involved in the commission of offence in any way then it cannot claim exemption from liability;
- Or upon receiving actual knowledge about any unlawful content the intermediary fails to remove the content alleged to be infringing.[83]

The precise meaning of 'actual knowledge' is unclear upon a bare reading of the statute – it is not defined in the IT Act,[84] and it remains unclear, for example, whether a notice from any private party would automatically imply that the intermediary under question now has 'actual knowledge' of the unlawful content. This is a standard discussed in more detail in the Intermediaries Guidelines, which also uses the 'actual knowledge' standard.

2. Information Technology (Intermediaries Guidelines) Rules, 2011

The Central Government notified the Intermediary Guidelines on April 11th, 2011, in exercise of the powers conferred by Section 87(2)(zg) read with Section 79(2) of the Information Technology Act, 2000. The most significant part of these rules is their definition of the term 'due diligence' as used within section 79(2) (c) of the IT Act.

The 'due diligence' obligations of intermediaries under the Intermediary Guidelines[85] include three broad categories of requirements that are relevant: (a) the publication of certain rules, policies and user agreements; (b) the obligation not to knowingly host, publish, or transmit infringing information; and (c) the obligation to take down infringing information upon receiving actual knowledge of it.

i. Publication of Rules, Policies, and Terms and Conditions

Intermediaries are required to publish rules and regulations, privacy policies, and user agreements,[86] which appears to be enforced through self-regulation.[87] The Intermediary Guidelines do, however, set out fairly detailed broad terms that need to be a part of the intermediaries' private agreement with users. The user agreements, rules, and policies must forbid the user from hosting, publishing, displaying, transmitting, or sharing any information:[88]

[82]The Information Technology Act, 2000, § 79, cl. 3(a).
[83]The Information Technology Act, 2000, § 79, cl. 3(a).
[84]Pritika Rai Advani, *Intermediary Liability in India*, XLVIII (50) EPW 120, 125 (Dec. 2013).
[85]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3.
[86]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3, cl. 1.
[87]John Braithwaite, *Enforced Self-Regulation: A New Strategy for Corporate Crime Control*,80(7) MICH. L. REV. 1466 (1982).
[88]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3, cl. 2.

- That is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful or racially, ethnically objectionable, disparaging, or relating to or encouraging money laundering or gambling,
- Harms minors in any way;
- Impersonates another person;
- Belongs to another person and to which the user does not have any right;
- Infringes any patent, trademark, copyright, or other proprietary rights;
- Violates any law, among other things; or,
- Threatens the unity, integrity, defense, security, or sovereignty of India, friendly relations with foreign states, or a public order, or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting to any other nation.

ii. Hosting, Publishing, Transmitting, or Modifying Infringing Information

The intermediary is also required to refrain from *knowingly* hosting, publishing, transmitting, or modifying any information prohibited under Rule 3(2)[89] (as listed in 'a' above).

Concerns were raised about the ambiguity of these terms, since none of them are defined in the IT Act or in the Intermediary Guidelines. In response, the Parliamentary Standing Committee on Subordinate legislation has already asked the Ministry of Communications and Information Technology to incorporate definitions of all these terms within the Intermediary Guidelines, and to ensure that the Guidelines do not end up creating any new category of offence.[90]

iii. Disabling Prohibited Information Upon 'Actual Knowledge'

The intermediary, upon receiving actual knowledge, whether on its own or whether through a written communication from an affected person that infringing information is being stored, hosted, or published on its computer system, is obligated to 'disable' such information within 36 hours of obtaining such knowledge.[91]

This last requirement effectively creates a notice and takedown regime. Although the Ministry insists that this is a self-regulatory regime,[92] a study conducted by the Centre for Internet and Society, Bangalore has demonstrated that intermediaries over-comply and tend to take down even legitimate information when they are sent a notice.[93]

The Ministry of Communication and Information Technology argued before the Parliamentary Standing Committee that the requirement to 'act' within 36 hours means that intermediaries have

[89]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3, , cl. 3.
[90]Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013), ¶ 25-26, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf.
[91]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3, cl. 4.
[92]Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013), ¶ 49, 55, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf.
[93]Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, Centre for Internet & Society (Apr. 10, 2012), *available at* http://cis-india.org/Internet-governance/intermediary-liability-in-india.

to respond to and acknowledge the complaint within 36 hours of receiving it, and initiate appropriate action. Upon the Parliamentary committee's insistence that this position should be clarified in the rules, the ministry issued an official clarification that states this position.[94] It said that while the Grievance Officer acting on behalf of the intermediary must act on the complaint expeditiously, the maximum time for redress is one month from the date on which the complaint was received, in accordance with Rule 3(11).

Subsequently, on March 23rd, 2012, a motion to annul guidelines was moved in the Rajya Sabha (Upper House of the Parliament). The annulment was defeated.[95] However, the rules have been challenged before the Supreme Court of India.

3. Blocking Orders Under the IT Act

Section 69A of the IT Act empowers the Central Government to direct the blocking of access to online information, and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 contain the procedure to be followed[96] for blocking access to information. As will be apparent from reading the procedure below, there are few external checks and balances in this process: the different stages of review of blocking orders are all conducted by committees or individuals who are a part of the executive branch of the government, and since there is a prohibition on disseminating information about the blocking orders,[97] the entire process is very opaque.

These blocking orders may be directed at any government agency or intermediary. Although these orders can, in theory, be directed at any intermediary (including ISPs and online intermediaries), sources tell us that they are typically directed at telecommunication companies and ISPs. However, this is not exclusively so, since it appears that the government has issued section 69A blocking orders to online intermediaries.[98]

The language used in the IT Act does not permit blocking orders to be issued arbitrarily. Under section 69A, it is only when the Government is of the view that it is "necessary or expedient" so to do in the interest of "sovereignty and integrity of India, defense 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",[99] that it can direct blocking access to information generated, transmitted, received, stored, or hosted in any computer resource.[100]

---

[94]Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India, Clarification on The Information Technology (Intermediary 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(1).pdf.

[95]Anupam Saxena, *Motion For Annulment of India's IT Rules Defeated In Rajya Sabha; IT Minister Promises Consultation*, Medianama (May 18, 2012), http://www.medianama.com/2012/05/223-motion-for-annulment-of-india%E2%80%99s-it-rules-defeated-in-rajya-sabha-it-minister-promises-consultation/.

[96]The Information Technology Act, 2000, § 69A, cl. 2.

[97]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 16; *Verizon Releases Transparency Report* (Jan, 22, 2014), http://newscenter.verizon.com/corporate/news-articles/2014/01-22-verizon-releases-transparency-report/.

[98] http://164.100.47.132/LssNew/psearch/QResult15.aspx?qref=151935.

[99]The Information Technology Act, 2000, § 69A, cl. 1.

[100]The Information Technology Act, 2000, § 69A, cl. 1.

The reasons for the blocking must be recorded in writing.[101] Intermediaries who do not comply with the requests can be punished with imprisonment of up to seven years and are also liable to pay a fine.[102]

Individuals cannot directly request the blocking of access to any content[103] and need to send their complaints to the "nodal officers" of the organizations in question.[104] The term "organizations" in India means ministries and departments of the Central Government, or any of the State, Union Territory, or other Central Government agency that may be notified.[105] After examining the complaint and being satisfied with the need to block access, the organization may forward the complaint through its nodal officer to the "Designated officer,"[106] who is appointed by the Central Government and is the only person under the act who can issue directions for blocking (apart from the courts).

All the requests received by the Designated Officer are to be examined by a committee[107] (referred to as 'Blocking Order Committee' in this paper) consisting of the designated officer and representatives from the ministries of Law and Justice, Home Affairs, Information and Broadcasting, and the Indian Computer Emergency Response Team (CERT-In)[108] within seven days.[109] The committee is required to examine the request and determine whether it is covered under the grounds mentioned in Section 69A and should give specific recommendations on the request received.[110] The designated officer is required to make an effort to identify the person to whom the information in the complaint belongs or the intermediary who has hosted the information, and give this individual or entity the opportunity to be heard.[111] The recommendations of the Blocking Order Committee are presented to the Secretary of the Department of Technology for approval.[112] This process may be bypassed in the event of an emergency, in which case the designated officer is authorized to examine the request and submit

[101]The Information Technology Act, 2000, § 69A, cl. 1.
[102]The Information Technology Act, 2000, § 69A, cl. 3.
[103]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 6.
[104]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 4.
[105] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 2, cl. g. "Organisation" means – (i) Ministries/Departments of Government of India; (ii) State Governments and Union Territories; (iii) Any other entity as may be notified in Official Gazette by the Central Government.
[106]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 3.
[107]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 7.
[108]Constituted under the Information Technology Act, 2000, § 70B.
[109]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 11.
[110]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 8.
[111]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 8, cl. 1, cl. 2 and cl. 3.
[112]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 8, cl. 5 and cl. 6.

his recommendations to the Secretary,[113] who, if satisfied, can pass an interim decision to block access through a written and reasoned order.[114] However, this request has to be brought before the Blocking Order Committee within 48 hours of the blocking order by the Secretary[115] and on the basis of the recommendations of the committee, the Secretary may revoke his/her approval and ask for the blocked content to be unblocked.[116] It is important to note that by the time blocking orders come before the Review Committee, the content under question is already blocked in India. This raises questions about how the committee is able to view the actual content, which may include videos, blocked during its review.

The rules also provide separately for a Review Committee,[117] which is mandated to meet at least once in every two months to review whether the directions issued for blocking are in accordance with Section 69A(1).[118] If the Review Committee is of the opinion that the orders issued are not in conformity with Section 69A(1), it may set aside the blocking order and ask for the information to be unblocked.[119] It is important to note that by the time blocking orders come before the Review Committee, the content under question is already blocked in India. This raises questions about how the committee is able to view the actual content, which may include videos, blocked during its review.

The Review Committee for blocking orders does not have to review orders from Indian courts asking for the blocking of any information. In these situations, the designated officer is required to submit a certified copy of the court order to the Secretary and initiate action as directed by the court.[120]

4. Interception Under the IT Act

Section 69 of the Information Technology Act requires intermediaries to extend all facilities and technical assistance to intercept, monitor or decrypt information, provide information stored in a computer or provide access to a computer resource, when called upon to do so by the agency of the appropriate government as contemplated in Section 69. This clearly extends to online intermediaries. As stated above, intermediaries that fail to meet these obligations may be punished with imprisonment of up to seven years.[121]

---

[113]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 9, cl. 1.
[114]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 9, cl. 2.
[115]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 9, cl. 3.
[116]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 9, cl. 4.
[117] The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 2, cl. (i) read with the Indian Telegraph Rules, 1951, r. 419A.
[118]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 14.
[119]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 14.
[120]The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, r. 10.
[121]The Information Technology Act, 2000, § 69, cl. 4.

The power to order interception rests with both the Central Government and the State Governments. Officers specially authorized have the power to order interception, monitoring, or decryption of data under specified circumstances. An interception order can be passed if it is necessary or expedient to do so in the interest of sovereignty or integrity of India, the defense of India, the security of State, friendly relations with foreign states, a public order, for preventing incitement to the commission of a cognizable offence relating to the above, or for investigation of any offence.[122] Interception of online communication is subject to the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, and has to follow the process detailed in the legislation.

The order for interception must be issued by a competent authority[123] designated as the Secretary in charge of the Ministry of Home Affairs for Central Government,[124] or the Home department for States or Union Territories[125] as may be applicable. The competent authority is required to consider whether it is possible to acquire the necessary information by other means and to order interception only if this is not possible.[126] An interception order may only remain in force for up to a period of 60 days and cannot be extended beyond a total of 180 days.[127]

Interception orders are conveyed to intermediaries by a designated nodal officer who authenticates them and conveys them to the designated person within the intermediary[128] along with a written request to facilitate the interception.[129] The designated officer of the intermediary or person in charge[130] must acknowledge the interception order within two hours of receipt and has to facilitate interception.[131] Intermediaries need to send interception requests every 15 days for authentication to the nodal officer of government agency.[132]

[122]The Information Technology Act, 2000, § 69, cl. 1.
[123]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 3.
[124]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 2(d)(i).
[125]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 2(d)(ii)
[126]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 8.
[127]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 11.
[128]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 12.
[129]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 13.
[130]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 14.
[131]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 15.
[132]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 18.

Intermediaries are required to destroy all the records within a period of two months following the discontinuance of interception or monitoring, unless they are required for any ongoing investigation, criminal complaint, or legal proceedings.[133]

Section 69B of the IT Act empowers the Central Government to authorize a government agency to monitor and collect attributes of the content, such as the time and date of its sending, size, duration, route (including the location and identities of the points of origin and destination),[134] and the type of underlying service ("traffic data") in order to enhance cyber security or for identification analysis and the prevention of intrusion or spread of computer containment in India.[135] Intermediaries are obligated to provide technical assistance and extend all facilities to the authorized agency,[136] or risk imprisonment for up to seven years.[137] These detailed procedures and other safeguards for such orders are listed in the Information Technology (Procedures and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009.

Like the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, these rules require an order from a competent authority. This order may however be issued for a range of cyber security purposes including, tracking cyber security breaches or incidents, identifying or tracking any person who has breached, or who is suspected of having breached or being likely to breach, cyber security,[138] and must contain the reasons issuing such direction.[139] A nodal officer has to receive the order and send it to the designated officer of the intermediary.[140] These safeguards are very similar to the safeguards outlined above for interception of information.

These rules also place obligations on the intermediary or the person in charge to put in place adequate checks to ensure that unauthorized monitoring does not take place[141] and make the intermediary liable for the actions of its employees in the case of unauthorized monitoring or the collection of data.[142]

C. The Copyright Act, 1957

The safe harbor protection provided to intermediaries under the IT Act is subject to section 81 of the IT Act which states that nothing contained in the IT Act shall restrict any person from

[133]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r. 23(2).
[134]The Information Technology Act, 2000, § 69B, explanation (ii) .
[135]The Information Technology Act, 2000, § 69B, cl. 1.
[136]The Information Technology Act, 2000, § 69B, cl. 2.
[137]The Information Technology Act, 2000, § 69B, cl. 4.
[138]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 3(2).
[139]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 3(3).
[140]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 4(2).
[141]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 5.
[142]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 6.

exercising any right conferred under the Copyright Act.[143] If not for the safe harbor protection contained within the Copyright Act, intermediaries could be held liable under Section 51(a)(ii) for secondary copyright infringement: under this, any person who provides any place to be used for communication of work to the public for profit, where such communication constitutes a copyright infringement, may be held liable for the infringement.[144] This would ordinarily open intermediaries to liability in cases where they store information on their servers and/or transmit it onwards, particularly when the profit from advertising in relation to infringing content.[145]

However, a safe harbor has been included via section 52 of the Copyright Act, which states that "transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public" shall not amount to copyright infringement; and that "transient or incidental storage of a work or performance for the purpose of providing electronic links, access or integration, where such links, access or integration has not been expressly prohibited by the right holder" is also not infringement, unless the intermediary has reasonable grounds for believing that such storage is of an infringing copy. It has been made clear that the immunity offered under section 52 is not meant to extend to deliberate storage of infringing information.[146] However the problem here is the interpretation of what amounts to reasonable grounds for belief that an intermediary is storing infringing content; the judiciary has, in the past, seen the insertion of algorithm-generated advertisements as an indication of knowledge of infringement.[147] Commentators point out that this standard will need to be discarded since it confuses physical space with the manner in which the Internet works.[148]

Like the IT Act, the Copyright Act makes its immunity for intermediaries conditional: the proviso to Section 52(1)(c) requires intermediaries to refrain from facilitating access to potentially infringing content for 21 days upon receiving a written complaint from the copyright owner about infringement that is taking place the transient or incidental storage that constitutes infringement. However, access to the content may be restored after 21 days unless a court order requiring the take down is received within a period of 21 days. This creates a notice and takedown regime where content needs to be removed at the behest of individual complaints. Unlike the IT Act, however, the Copyright Act explicitly authorizes the restoration of content in cases where a court has not endorsed the complaint.

This notice and takedown regime is mapped out more clearly in Rule 75 of the Copyright Rules of 2013. The rights holder has to give written notice[149] to the intermediary, including details about the description of work for identification,[150] proof of ownership of original work,[151] proof

[143]This position is affirmed by Super Cassettes Industries Ltd v. Myspace Inc, M.I.P.R. 2011 (2) 303 (India).
[144] The Copyright Act, 1957, § 51, cl. a(ii).
[145] Super Cassettes Industries Ltd v. Myspace Inc, M.I.P.R. 2011 (2) 303 (India); Aditya Gupta, *The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under the Indian Laws- The Road Ahead*, 15 J. I.P.R. 35, 37 (2010).
[146]Ananth Padmanabhan, *Give Me My Space and Take Down His*, 9 I.J.L.T 2 (2013), *available at* http://www.ijlt.in/archive/volume9/Ananth%20Padmanabhan.pdf.
[147] Super Cassettes Industries Ltd v. Myspace Inc, M.I.P.R. 2011 (2) 303 (India).
[148]Ananth Padmanabhan, *Give Me My Space and Take Down His*, 9 I.J.L.T 15-16 (2013), *available at* http://www.ijlt.in/archive/volume9/Ananth%20Padmanabhan.pdf.
[149] The Copyright Rules, 2013, r. 75, cl. 2.
[150] The Copyright Rules, 2013, r. 75, cl. 2(a).

of infringement by work sought to be removed,[152], the location of the work[153] (which would be the specific URL), and details of the person who is responsible for uploading the potentially infringing work (if available).[154] Upon receiving such a notice, the intermediary has to disable access to such content within 36 hours.[155] In a departure from the Intermediaries Guidelines, and in a positive move for transparency, intermediaries that host content are required to display reasons for disabling access to anyone trying to access the content.[156] The intermediary is permitted, but not required, to restore the content after 21 days if no court order is received to endorse its removal.[157] It is then not required to respond to further notices from the same complainant about the same content at the same location.[158]

However, the regime under the Copyright Act is also not without its problems. Critics have objected to the narrowness of "transient or incidental storage," which is necessary to claim immunity from liability under the safe harbor provision. They have also objected to the process under Rule 75, pointing out that it should have required the intermediary to notify the person who uploaded or created the content, creating an opportunity for a response that will enable the intermediary to let the content remain as is.[159]

Also of concern are the vaguely worded court orders increasingly issued in the context of copyright issues. These "John Doe" orders – or "Ashok Kumar" orders as they are called in India – are used by copyright owners to get ex parte injunctions against unknown parties.[160] There was a point at which these orders were so broad that they could be interpreted as creating a positive obligation on all intermediaries to proactively remove the questionable content. An example of the language used is, "For the forgoing reasons, defendants, their partners, proprietors…servants, agents, representatives…other unnamed and undisclosed persons, are restrained from communicating without license or displaying, releasing, showing, uploading, downloading, exhibiting, playing, and/or defraying the movie "DEPARTMENT" in any manner without a proper license from the plaintiff."[161]

---

[151] The Copyright Rules, 2013, r. 75, cl. 2(b).
[152] The Copyright Rules, 2013, r. 75, cl. 2(c).
[153] The Copyright Rules, 2013, r. 75, cl. 2(d).
[154] The Copyright Rules, 2013, r. 75, cl. 2(e).
[155] The Copyright Rules, 2013, r. 75, cl. 3.
[156] The Copyright Rules, 2013, r. 75, cl. 4.
[157] The Copyright Act, 1957, § 52(1), proviso.
[158] The Copyright Rules, 2013, r. 75, cl. 6.
[159] Apar Gupta, *Copyright Rules, 2013 and Internet Intermediaries*, Indian Law and Technology Blog (March 22, 2013); http://www.iltb.net/2013/03/copyright-rules-2013-and-Internet-intermediaries/; Chaitanya Ramachandran, *A Look at the New Notice and Takedown Regime under the Copyright Rules 2013*, Spicy IP (Apr 29, 2013), http://spicyip.com/2013/04/guest-post-look-at-new-notice-and.html.
[160] Lawrence Liang, *Meet Ashok Kumar the John Doe of India; or The Pirate Autobiography of an Unknown Indian*, Kafila (May 18, 2012), http://kafila.org/2012/05/18/meet-ashok-kumar-the-john-doe-of-india-or-the-pirate-autobiography-of-an-unknown-indian/.
[161] Viacom 18 Motion Pictures v. Jyoti Cable Network and Ors, C.S.(OS) 1373/2012 (May 14, 2012), High Court of Delhi (India).

The Madras High Court in *M/s. R.K. Productions Pvt. Ltd. vs. Bharat Sanchar Nigam Limited & 19 others*,[162] clarified in June 2012 that an earlier interim injunction was granted only in relation to a particular URL where the infringing movie is hosted, and not to of the entire website (addressing the overbroad blocking that was taking place by ISPs in response to such injunctions). Further, the applicant is directed to inform the respondents/defendants about the particulars of URL where the infringing movie is kept. On such receipt of the particulars of the URL in question from the plaintiff/applicant, the defendants shall take necessary steps to block such URLs within 48 hours. The following year, in December 2013, the Delhi High Court passed an Ashok Kumar order, an ad interim ex parte injunction that applied to "unnamed and undisclosed persons" in relation to the display, duplication, and distribution of the film 'Dhoom 3.'[163] Recently, the Delhi High Court issued such an injunction prohibiting 472 websites[164] and other unknown ones from broadcasting 2014 FIFA World Cup matches, which it then reduced to a list of 219 upon an objection that several of the websites on the list did not belong there.[165]

III. Impact Assessment

The legal framework governing the liability of Internet intermediaries in India has to remain consistent with the Indian Constitution.[166] This means that the statutory framework under which intermediaries are liable to block, take down, intercept, and monitor content may be challenged if it violates the right to the freedom of speech and expression,[167] or the right to privacy (as read into the right to life and personal liberty,[168] the right to the freedom of speech, and expression by the judiciary[169]) granted by the Constitution. The regulatory framework is also subject to administrative law principles, derived largely from common law; meaning rules, notifications, and actions arising from legislations must remain within the scope of their parent statute and the constitution[170] and cannot usurp any function that rightfully belongs to the legislature.[171]

---

[162] *M/s. R.K. Productions Pvt. Ltd.* v. *Bharat Sanchar Nigam Limited & 19 Others*, C.S. (OS) 208/ 2012 (June 22, 2012), The High Court of Judicature at Madras (India).

[163] *Yash Raj Films Pvt Ltd* v. *Cable Operators Federation of India and Ors*, C.S.(OS) 2335/2013 (Dec. 2, 2013), High Court of Delhi (India).

[164] *Multi Screen Media Pvt Ltd* v. *Sunit Singh and Ors*, CS(OS) 1860/2014 (June 23, 2014), High Court of Delhi (India).

[165] Nikhil Pahwa, *World Cup 2014: 219 websites blocked in India, after Sony complaint*, Medianama (Jul 7, 2014), http://www.medianama.com/2014/07/223-world-cup-2014-472-websites-including-google-docs-blocked-in-india-following-sony-complaint/.

[166] India Const.

[167] India Const. art.19, cl. 1(a).

[168] India Const. art. 21.

[169] Kharak Singh v. State of UP, A.I.R. 1963 S.C. 1295 (India); Gobind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148 (India); R Rajagopal v. State of Tamil Nadu, A.I.R. 1995 S.C. 264 (India),¶ 9; District Registrar &Collector v. Canara Bank, A.I.R. 2005 S.C. 186 (India), ¶ 39.

[170] Indian Express Newspapers (Bombay) Pvt. Ltd. v. Union of India A.I.R. 1986 S.C. 515 (India).

[171] Agricultural Market Committee v. Shalimar Chemical Works Ltd A.I.R. 1997 S.C. 2502 (India); Ujwala Uppaluri, *Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011*, CIS India Blog (Jul. 16, 2012, 09:45 AM), http://cis-india.org/Internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules.

The technology actually used by intermediaries has had visible effects on speech,[172] and has resulted in over-blocking in the past. It does, however, appear that regulators take into account market concerns – these concerns are increasingly reflected in reports that discuss the formulation of the regulatory regime and in arguments made by the Government of India before the Supreme Court of India.[173]

The narrative in the earlier parts of this paper mapped out the different kinds of liability to which online intermediaries are subject in India. This includes criminal liability for several kinds of content, including content that is defamatory,[174] obscene,[175] or amounts to contempt of court.[176] The Indian Penal Code uses gatekeeper liability to regulate unlawful speech,[177] and this can make operations risky for intermediaries without immunity from liability under section 79 of the IT Act. Recent interpretations of the law by the Indian Supreme Court indicate that intermediaries may find themselves at risk despite the immunity offered by the IT Act. In January 2015, the Supreme Court passed an interim order in an ongoing case, requiring Google, Yahoo, and Microsoft to refrain from advertising or sponsoring any advertisement which would violate Section 22 of the Pre-Conception and Pre-Natal Diagnostic Techniques Act, 1994.[178] This interpretation seems to accept the argument made by the Ministry of Information and Communications that search engines, as intermediaries under the IT Act, owing to their 'due diligence' obligations, must block all content that breaches Indian laws. However since this is merely an interim order, there remains some chance that the Supreme Court will change its mind on the subject by the time the final judgment is delivered.

If the interim order represents the Supreme Court's stand on this subject, it may undo the beneficial effects of safe harbor protection for search engines. Intermediaries may have very little clarity about the kinds of content they need to weed out, given the different kinds of speech criminalized by multiple Indian statutes (indicative list in the table in Annexure 1). This makes intermediaries who exercise editorial control particularly vulnerable. The IT Act adds to the list

[172]Anupam Saxena, *Over 200 sites blocked in India after Sony's piracy complaint: Report*, Times of India (Jul. 7, 2014), http://timesofindia.indiatimes.com/tech/tech-news/Over-200-sites-blocked-in-India-after-Sonys-piracy-complaint-Report/articleshow/37961214.cms;OpenNet Initiative, Country Profile: India 304 (Aug. 9, 2012), *available at* http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-india.pdf.

[173]Standing Committee on Information Technology 2007-08, Parliamentary Report on the Information Technology (Amendment) Bill, 2006, 16 (Sept. 7, 2007), *available at* http://www.prsindia.org/uploads/media/Information%20Technology%20/scr1198750551_Information_Technology.pdf; Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013), ¶ 77, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf; Sarvjeet Singh, *A Blanket Ban on Porn will violate Articles 19 & 21 of the Constitution: Government informs the Supreme Court*, CCG at NLUD Blog (May 5, 2014), http://ccgnludelhi.wordpress.com/2014/05/05/a-blanket-ban-on-porn-will-violate-articles-19-21-of-the-constitution-government-to-the-supreme-court/.

[174]The Indian Penal Code, 1860, § 499.

[175]The Indian Penal Code, 1860, § 292, The Information Technology Act, 2000, § 67.

[176] The Contempt of Courts Act, 1971, §§ 2, cl. c and 12.

[177]Chinmayi Arun, N.U.J.S. L. Rev. (forthcoming 2014)

[178] Sabu Mathew George v. Union of India, W.P. (C) No. 341/2008, interim order (Jan. 28, 2015), Supreme Court of India (India)

of criminalized speech, creating new categories of offences punishable with imprisonment ('grossly offensive' information,[179] for example).

Online intermediaries with no editorial control are also in a precarious position, despite their greater access to immunity from liability. The safe harbor protection granted to them under the IT Act is conditional upon the intermediaries observing "due diligence,"[180] and on their removing unlawful content upon receiving "actual knowledge" of such content.[181] Interestingly, one outcome of section 79 has been that online intermediaries are immune from liability in contexts in which bookstores, traditional media, and publishing houses would have been found to be liable (such as hosting obscene content).[182] Even online intermediaries with immunity are required to refrain from *knowingly* hosting, publishing, transmitting, or modifying any information prohibited under Rule 3(2).[183] This list of prohibited information consists of a very wide range of content including content that is "grossly harmful," "harassing," "pornographic," "pedophilic," "libelous," "invasive of another's privacy," "hateful," "racially, ethnically objectionable," and "disparaging."[184] Many of these are categories of content that are not defined in Indian law at all.

Terms like 'defamatory' and 'obscene',[185] which are actually defined in other pieces of Indian legislation, are not defined in the Intermediary Guidelines. While this might not be a hardship for large online intermediaries like Google or Facebook that have the resources to hire a legal team, a start-up or small online intermediary may struggle to acquire the legal expertise to ascertain what is meant by all the terms listed in Rule 3. This makes Rule 3 an opaque and inaccessible rule from the intermediaries' perspective. Compliance with such an unclear standard is difficult. The Parliamentary Standing Committee on subordinate legislation has recommended that all these terms which are not defined in the IT Act be defined in the Intermediary Guidelines for the convenience of the intermediaries and the general public.[186] If this recommendation were executed, it would make for a more transparent rule.

Intermediaries that are subject to the licensing system in India have to contend with the added burden of onerous requirements that cover blocking, interception, and monitoring.

The architectural constraints of the Internet are becoming apparent to the government, which has moved from its command-control approach to the position that comprehensive and guaranteed blocking of information is impossible.[187] The current regulatory regime tries to leverage

[179]The Information Technology Act, 2000, § 66A.
[180]The Information Technology Act, 2000, § 79.
[181]The Information Technology Act, 2000, § 79.
[182]Chinmayi Arun, N.U.J.S. L. Rev. (forthcoming 2014).
[183]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3.
[184]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3.
[185]The Information Technology (Intermediaries guidelines) Rules, 2011, r. 3.
[186]Standing Committee on Subordinate Legislation, Thirty First Report on The Information Technology Rules (March 21, 2013), ¶ 25, *available at* http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf.
[187] Sarvjeet Singh, *A Blanket Ban on Porn will violate Articles 19 & 21 of the Constitution: Government informs the Supreme Court*, CCG at NLUD Blog (May 5, 2014), http://ccgnludelhi.wordpress.com/2014/05/05/a-blanket-ban-on-porn-will-violate-articles-19-21-of-the-constitution-government-to-the-supreme-court/; Sarvjeet Singh, *Cannot Block all Pornographic Material over the Internet: Centre informs the SC*, CCG at NLUD Blog (Aug 29, 2014),

intermediaries' existing capabilities by requiring them to make reasonable efforts to develop terms and conditions, as well as technological filters to regulate user-behavior. This looks like the beginnings of enforced self-regulation since it leaves the choice of technology and user agreements to the intermediaries after specifying the minimum terms or standards that need to be incorporated. However, it is not clear whether and how compliance is monitored in this context.

As it stands, under-resourced start-up companies may not be able to put in place a complex system to meet these standards, and making it risky to enter the market.[188] A Global Network Initiative study concluded that online intermediaries are burdened by costs and risks associated with the current legal regime in India, and that this regime has had a detrimental impact on established businesses and new ventures.[189]

There is very little transparency, and therefore limited accountability, in the process followed while blocking, intercepting, or monitoring content. This is detailed in the sections below.

A. Government-Ordered Blocking of Content

The Blocking Rules permit government agencies to ask for content to be blocked. Although these requests are most frequently directed at telecommunication companies and Internet service providers, they are also sent to online intermediaries from time to time. For example, social networking sites were asked to comply with court orders by blocking 8 URLS in 2010, 21 URLS in 2011, 352 URLs in 2012, and 1299 URLS from January 2013-2014.[190]

The government-ordered blocking process under the Blocking Rules is shrouded in secrecy – Rule 16 of the Blocking Rules requires that blocking requests and implementation be kept confidential. The effect is that the government is able to refuse to give out information about blocking,[191] and companies are restricted from making disclosures in this context. This is the reason that the January 2014 Verizon transparency report did not disclose the number of blocking requests from the Indian government, and explained that Indian law did not permit Verizon to make this disclosure.[192]

---

http://ccgnludelhi.wordpress.com/2014/08/29/cannot-block-all-pornographic-material-over-the-Internet-centre-informs-the-sc/.

[188] Martin Hvidt Thelleet. al., *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose*, Copenhagen Economics (2014), *available at* http://www.globalnetworkinitiative.org/sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf.

[189] Martin HvidtThelleet. al., *Closing the Gap – Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose*, Copenhagen Economics (2014), *available at* http://www.globalnetworkinitiative.org/sites/default/files/Closing%20the%20Gap%20-%20Copenhagen%20Economics_March%202014_0.pdf.

[190] Reply by Mr. Kapil Sibbal, Minister of Communications & Information Technology, Government of India to Mr. Baijayant Panda, Member of Parliament, Starred question number 318 on Objectionable Content on Websites, LokSabha (Feb. 12, 2014), http://164.100.47.132/LssNew/psearch/QResult15.aspx?qref=151935.

[191] Reply to the RTI Application filed by Sarvjeet Singh at Centre for Communication Governance at National Law University, Delhi to the Department of Electronics and Information Technology, E-Security Division, (March 25, 2014).

[192] *Verizon Releases Transparency Report*, (Jan. 22, 2014), http://newscenter.verizon.com/corporate/news-articles/2014/01-22-verizon-releases-transparency-report/.

Since the system is opaque and does not require judicial or third party review or oversight at any point, it is reasonable to deduce that this may lead to reduced accountability. Government agencies ask for online content blocking through a process that is authorized, executed, and reviewed by the executive. Information about this blocking is not proactively disclosed by the government and cannot be disclosed by the intermediaries owing to Rule 16. The only mechanism to obtain the figures appears to be if a Member of Parliament asks for them in Question Hour.[193] Even the author or creator of the content, who might in theory have contested a blocking order on grounds of his/her constitutional free speech rights, has no way of contesting it since no reasons or notifications about the blocking of content need to be given to the creators or the audience of content.

In addition to the blocking requests that come from government agencies, court-ordered blocking of content also takes place under the IT Act. There is a Delhi High Court judgment confirming that 69A-blocking orders were sent to Google India Private Ltd. over the 'Innocence of Muslims' videos on YouTube.[194] 190 URLS were blocked over the videos as the Department of Electronics & Information Technology implemented orders from courts in Budagam, Ganderbal, Baramula, Srinagar, Anantnag in Jammu & Kashmir and courts at Akola, Bhiwadi, Mumbai, and Delhi.[195] 52 URLS of these videos were blocked under the Blocking Rules.[196]

Even the court orders, which are public documents in theory, are inaccessible in practice since many of them are obtained from remote regional courts. This also raises questions about how an intermediary might find the resources to travel to these locations and challenge any unreasonable blocking requests. Finally, since there is no mechanism to verify that each of the blocked URLS do in fact contain the content complained of, there is extensive potential for misuse of the blocking process.

At a meeting of the Cyber Regulation Advisory Committee, the Minister of Communications and Information Technology asked the Internet and Mobile Association of India, which is an industry association, to monitor and prepare a list of pornographic sites for blocking by the ISPs. The minister has suggested the need to understand United Kingdom system of installation of filtering software on home computers so that this may be replicated in India with modifications for the "Indian context."[197]

---

[193] Reply by Mr. Kapil Sibbal, Minister of Communications & Information Technology, Government of India to Mr. Baijayant Panda, Member of Parliament, Starred question number 318 on Objectionable Content on Websites, LokSabha (Feb. 12, 2014).

[194]Mohd. Amanullah & Ors. v. Union Of India &Ors., W.P. (C) No. 6325/2012 (Oct. 10, 2012), High Court of Delhi (India).

[195]Maulana Mahmood Asad Madani v. Union of India and Ors., W.P. (C) 7545/2012 (Jan. 24, 2013), High Court of Delhi (India).

[196]Maulana Mahmood Asad Madani v. Union of India and Ors., W.P. (C) 7545/2012 (Jan. 24, 2013), High Court of Delhi (India).

[197] Minutes of Meeting of the Cyber Regulation Advisory Committee, ¶ 14, (5 Sept. 2014), *available at* http://deity.gov.in/sites/upload_files/dit/files/Min-CRAC-5%20Sept.pdf; Jayadevan PK & Neha Alawadhi, *Government asks internet service companies to block pornography sites, upgrade systems,* THE ECONOMIC TIMES (Nov. 11, 2014), http://articles.economictimes.indiatimes.com/2014-11-11/news/55990473_1_internet-service-providers-internet-freedom-blocking-internet

This inclination towards blocking content is not, however, uniform within the Government. There are those who argue that filtering and blocking of content is a problematic solution. For example, a Secretary of the Ministry of Law and Justice stated in a Cyber Regulation Advisory Committee meeting[198] that, "it is not desirable to submit the plea to Supreme Court that it is difficult to filter or block pornography sites and we must try to evolve a solution."[199] Similarly, the Government has, in the past, told the Supreme Court that it is not technically feasible to block pornographic sites[200] and that doing so will be violation of Article 19 and 21 of the Indian Constitution.[201] It is, however, important to remember that this is not a consistent position and it is possible that the government will reverse its stance in the very same case once it comes up for hearing in February 2015.

B. Notice and Takedown

The safe harbor protection under section 79 of the IT Act is subject to the intermediary's removal of unlawful content immediately after receiving "actual knowledge" of it. The Intermediary Guidelines attempt to clarify what this phrase means, explaining that the intermediary could obtain such knowledge by itself or have such knowledge communicated to it by "an affected party in writing" or through an email signed by an electronic signature. After this, the intermediary is expected to "act within thirty six hours" to disable such information as it falls within the list of (undefined) prohibited content given in the Intermediary Guidelines. This has effectively created a notice and takedown regime for content.

The impact of these guidelines on intermediaries was demonstrated in a study conducted by the Centre for Internet & Society, Bangalore,[202] which tried sending frivolous notices to multiple intermediaries about perfectly legitimate content. The study found that intermediaries tend to remove even legitimate content in response to notices from private parties. A researcher sent take down notices to seven major intermediaries and found that six of these intermediaries over-complied. This offers some evidence to support the argument that the Intermediaries Guidelines might result in suppression of legitimate expression, since there is a visible chilling effect created by these guidelines. However the sample size for this study may be seen as problematic, and a larger investigation using the same method might be welcome.

The fact that intermediaries over-comply, disabling legitimate and legal content under the Intermediaries Guidelines is not surprising given the incentives created by the rules. Any failure to take down content places the intermediary at the risk of expensive litigation, but the rules do not require the intermediary to notify the author or user whose content has been taken down, or

---

[198] Established under the Information Technology Act, 2000, § 88.

[199] Minutes of Meeting of the Cyber Regulation Advisory Committee, ¶ 4, (5 Sept. 2014), *available at* http://deity.gov.in/sites/upload_files/dit/files/Min-CRAC-5%20Sept.pdf.

[200] Sarvjeet Singh, *Cannot Block all Pornographic Material over the Internet: Centre informs the SC*, CCG at NLUD Blog (Aug 29, 2014), http://ccgnludelhi.wordpress.com/2014/08/29/cannot-block-all-pornographic-material-over-the-Internet-centre-informs-the-sc/.

[201] Sarvjeet Singh, *A Blanket Ban on Porn will violate Articles 19 & 21 of the Constitution: Government informs the Supreme Court*, CCG at NLUD Blog (May 5, 2014), http://ccgnludelhi.wordpress.com/2014/05/05/a-blanket-ban-on-porn-will-violate-articles-19-21-of-the-constitution-government-to-the-supreme-court/.

[202] Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, Centre for Internet & Society (Apr. 10, 2012), *available at* http://cis-india.org/Internet-governance/intermediary-liability-in-india.

offer this speaker the right to defend his/her content or modify it such that it may legitimately stay online. The rules also do not contain any mechanism requiring intermediaries to make it clear to the audience that content has been taken down, making the entire system very opaque.

Bringing all these elements together, it is clear that the system for taking down content under the IT Act in India is very problematic because it (a) permits horizontal censorship by requiring intermediaries to respond quickly to any private citizen who may care to send them notice without any countervailing obligations towards authors or audiences; (b) obligates private intermediaries to make decisions about speech even when they are not performing an editorial function, and may lack the resources to make such determinations; and (c) ensures that there is no transparency at all about decisions to take down content, leading to a lack of accountability of private intermediaries for over-broad blocking and a lack of information based on which citizens may challenge particular instances of blocking.

The notice and takedown system under the Copyright Act might be marginally better in terms of transparency, since intermediaries are required to display a notice about why it was taken down.[203] The statute also permits (although it does not obligate) the intermediary to reinstate any content for which a court order is not received in 21 days.[204] This could, in theory, reduce the abuse of the notice and takedown system by private parties.

However this process is undermined to a great degree by the judiciary's practice of issuing ex parte 'John Doe' or 'Ashok Kumar' orders to disable allegedly infringing content. These orders would imply that the limitation on the period of the takedown would cease to apply. Critics point out that cases like *Multi Screen Media Pvt Ltd* v. *Sunit Singh*[205] indicate that the courts do not pay sufficient attention to the actual URLs that they are asked to block (the list of URLs had to be revised substantially; websites obviously wrongly named included Google Documents, which had to be removed from the original list).[206] Court-ordered blocks are only the tip of the iceberg. This is apparent when one considers for instance that *Multi Screen Media Pvt Ltd* v. *Sunit Singh*[207] is not Multi Screen Media's first sojourn into the realm content blocking. Google's transparency report for 2014 indicates that between February and July 2014, this company has made 77 removal requests to Google, covering a total of 27,624 URLs.[208] Out of these, 16,309 URLs were actually removed. In December 2014, 32 websites, including dailymotion.com, vimeo.com, and github.com were blocked as a result of a court order.[209] This led to controversy

[203] The Copyright Rules, 2013, r. 75, cl. 4.
[204]The Copyright Act, 1957, § 52(1), proviso; The Copyright Rules, 2013, r. 75, cl. 5.
[205]CS(OS) 1860/2014 (June 23, 2014), High Court of Delhi (India).
[206] Nikhil Pahwa, *World Cup 2014: 219 websites blocked in India, after Sony complaint*, Medianama (Jul 7, 2014), http://www.medianama.com/2014/07/223-world-cup-2014-472-websites-including-google-docs-blocked-in-india-following-sony-complaint/.
[207] CS(OS) 1860/2014 (June 23, 2014), High Court of Delhi (India).
[208]*Requests to remove content due to copyright violation by Multi Screen Media Private Limited*, Google Transparency Report (2014), http://www.google.com/transparencyreport/removals/copyright/owners/57964/Multi-Screen-Media-Private-Limited/.
[209] *Websites Blocked Following Court Order*, Press Information Bureau (Dec. 31, 2014) http://pib.nic.in/newsite/PrintRelease.aspx?relid=114259; http://cis-india.org/internet-governance/resources/2014-12-17_DoT-32-URL-Block-Order.pdf

owing to the apparent over-blocking of content.[210] After extensive negative publicity, the websites were unblocked.[211] The incident is a good illustration of the flaws of the court-ordered blocking system. The over broad blocking suggests that the judiciary may not have examined the contents of each URL and website on the list compiled for blocking.

Generally, in the period between July-December 2013, Google received 21 court orders for taking down content, affecting 118 items. It complied with 52% of these requests. It also received 133 requests affecting 422 items from other agencies (executive, police etc.) and complied with 23% of those requests.[212] These requests included one from an election candidate's representative for the removal of a YouTube video that allegedly connected the candidate with corrupt financial practices – Google denied this request since it not go through proper legal channels. Another such content removal request came from the local police and sought the removal of a blog post that contained content and pictures about a politician's sex scandal. This request was also denied, this time on grounds of the subjects of the blog post not being identifiable.[213]

During January-June 2014, Facebook restricted 4,960 pieces of content based on requests primarily by law enforcement officials and the Indian Computer Emergency Response Team.[214] During the same period, Twitter received no court orders and 5 requests from other agencies (executive, police etc.) to remove content. It complied with none of these requests, which involved 9 accounts.[215]

C. Interception of Information by Intermediaries

Section 69 of the Information Technology Act requires online intermediaries to extend all facilities and technical assistance to intercept, monitor or decrypt information, provide information stored in a computer, or provide access to a computer resource when called upon to do so by the government.

The interception of information under the IT Act follows a very detailed process in which attempts are made at various safeguards, such as designating senior officials for decision-

[210] Kim Arora, *Government blocks 32 websites to check ISIS propaganda,* The Times of India (Jan. 1, 2015), http://timesofindia.indiatimes.com/tech/tech-news/Government-blocks-32-websites-to-check-ISIS-propaganda/articleshow/45712815.cms; R. Jai Krishna, *India Orders Blocking of Websites for Alleged ISIS Content*, The Wall Street Journal (Jan. 2, 2015), http://www.wsj.com/articles/india-orders-blocking-of-websites-for-alleged-isis-content-1420032698; Jayadevan PK & Neha Alawadhi, *Government faces a firestorm of protests, decides to unblock some websites*, The Economic Times (Jan. 1, 2015), http://articles.economictimes.indiatimes.com/2015-01-01/news/57581476_1_websites-various-internet-service-providers-information-technology.

[211] Neha Alawadhi, *Government orders ISPs to unblock 32 websites, links*, The Economic Times (Jan. 10, 2015), http://economictimes.indiatimes.com/tech/internet/government-orders-isps-to-unblock-32-websites-links/articleshow/45829881.cms.

[212] *Requests to remove content from the Government of India,* http://www.google.com/transparencyreport/removals/government/IN/.

[213] *Requests to remove content from the Government of India- Explore Requests,* http://www.google.com/transparencyreport/removals/government/notes/?hl=en#authority=IN&period=Y2013H2.

[214] *Government Requests Report: India, https://govtrequests.facebook.com/country/India/2014-H1/*; *India tops Facebook's content restriction list*, The Economic Times (Nov. 5, 2014), http://articles.economictimes.indiatimes.com/2014-11-05/news/55798412_1_requests-facebook-january-june

[215] *Removal requests: India*, https://transparency.twitter.com/country/in.

making, creating review committees, and requiring intermediaries to check and only follow legitimately issued orders. However, at no point does it provide for third party oversight or transparency. The latter, in particular, may be far more effective in ensuring that no misuse of the system takes place than in relying on a busy senior official who may not have the time to properly judge the interception request, and are not accountable if they should end up authorizing an interception that they should not have.[216] Although the IT Act asks that interceptions not be authorized unless the information under question cannot be obtained by other means, it does not contain any procedural enforcement of this principle.

Online intermediaries are required to intercept information on the threat of imprisonment,[217] and they have to designate officers to meet the IT Act's detailed and cumbersome safeguards.[218] This process of designating a person and then ensuring that all the interception orders are received, are in the proper form, and are signed by the right parties may prove very difficult for new entrants.

Yahoo was actually fined 1.1 million Rupees (about US $22,000) when the company refused to hand over information related to about a dozen Yahoo IDs and IP addresses that the government wanted because it suspected these IDs were being used by Islamic terrorists or Maoists.[219] Yahoo refused the request, arguing that it was not made through the channels required by law, and that the fine was imposed by an entity (Controller of Certifying Authorities)[220] without any authority to impose it.[221] The fine was eventually retracted, but Yahoo was made to provide the information.[222]

Google received 2,513 user data requests regarding 4,401 accounts from the Indian Government between January and June 2013. Google handed over the information in 66% of the cases.[223] Facebook received a total of 3,598 requests regarding 4,711 accounts between July to December 2013 and it provided information in 53.56% of cases.[224] Twitter received 19 account information requests regarding 27 accounts and complied with 32% of these.[225]

In the absence of transparency, it is impossible for citizens to discover whether their information has been intercepted. As a result, they have no means at all of holding the state accountable for illegal interception of information.

---

[216]Chinmayi Arun, *Way to Watch*, Indian Express(June 26, 2013), http://archive.indianexpress.com/news/way-to-watch/1133737/.
[217]The Information Technology Act, 2000, § 69, cl. 4.
[218]The Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, r. 14.
[219]Controller of Certifying Authorities, available at http://cca.gov.in/rw/resource/CCA-ORDER-ISSUED-TO-YAHOO-DIGITALLTY-SIGNED.pdf?download=true.
[220] Appointed under The Information Technology Act, 2000, § 17(7).
[221]Yahoo India Pvt. Ltd. v. Union of India, W.P. (C) 6654/2011 (Sept. 14, 2011), High Court of Delhi.
[222]Yahoo India Pvt. Ltd. v. Union of India, W.P. (C) 6654/2011 (Sept. 14, 2011), High Court of Delhi; Chinmayi Arun and Ujwala Uppaluri, *Report on the Indian Surveillance Framework* (July 2014), prepared on behalf of iProbono for Privacy International.
[223]*Requests for user information from the Government of India* http://www.google.com/transparencyreport/userdatarequests/IN/.
[224]*Government requests report:* India, https://govtrequests.facebook.com/country/India/2013-H2/.
[225]*Information requests: India* , https://transparency.twitter.com/information-requests/2013/jul-dec.

IV. Cases currently before the Supreme Court[226]

A. Rajeev Chandrasekhar[227]

Rajeev Chandrasekhar, a member of the Rajya Sabha (the upper house of the Parliament of India) has filed a petition in the Indian Supreme Court challenging Section 66A of the Information Technology Act, 2000 and Rules 3(2), 3(3), 3(4) and 3(7) of the Information Technology (Intermediaries Guidelines) Rules, 2011 as violating Articles 14, 19, and 21 of the Indian Constitution.

1. Information Technology (Intermediaries Guidelines) Rules, 2011

The petition states that Rule 3(2) lists the various types of information that should not to be carried. This violates Article 14 of the Constitution, as these categories are arbitrary and overly broad. Moreover, the rules grant the private intermediary the right to subjectively assess objectionable content and create categories outside of the restrictions provided under Article 19.

Rule 3(4) of the guidelines provides the intermediary 36 hours to disable the information that is in contravention of Rule 3(2) when it receives such information on its own, or on the basis of information received. The petition argues that the period of 36 hours for removal of content is impractical and infeasible for intermediaries that process enormous quantities of data. The rules also require the intermediary to keep the offending information and associated records for at least 90 days, while Rule 3(7) calls upon the intermediary to provide any information or assistance to a Government agency seeking such information in writing. Both these rules violate the privacy under Article 21 of the constitution.

B. Common Cause[228]

Common Cause, an NGO along with senior Aam Aadmi Party leader and former Law Minister of Delhi Somnath Bharti has filed a writ petition in the Supreme Court of India arguing that Section 66A of the Information Technology Act, 2000, Section 69A of the IT Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 and Section 80 of the IT Act are in violation of Article 14, 19, and 21 of the Indian Constitution.

1. Section 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

The petition puts forth various administrative law arguments that Section 69A of the IT Act and the 2009 rules framed under it violate the Constitution. It argues that the rules do not offer the creator or author of the content with a reasonable opportunity to be heard before blocking the

---

[226] Sarvjeet Singh, *Cases that will define the contours of Free Speech over the Internet in India*, CCG AT NLUD BLOG (Dec 10, 2014), https://ccgnludelhi.wordpress.com/2014/12/10/cases-that-will-define-the-contours-of-free-speech-over-the-internet-in-india/.

[227] Rajeev Chandrasekhar v. U.O.I. & Anr., W.P. (C) No. 23 (2013) (India), *available at* https://drive.google.com/a/nludelhi.ac.in/file/d/0B3Do3-9ZtwCrWnFKdTdLeXMwWlU/view.

[228] Common Cause (A Regd. Society) & Anr. v. U.O.I., W.P. (C) No. 21 (2013) (India), *available at* http://www.commoncause.in/whatsNew/8writpetition.pdf.

content. Additionally, there is no scope for a post-decision hearing, nor is there any provision to appeal the blocking order under the rules.

C. Moutshut.com[229]

Moutshut.com, a user review website, has filed a petition before the Supreme Court of India challenging the Information Technology (Intermediaries Guidelines) Rules, 2011, claiming that it violates Articles 14, 19, and 21 of the Indian Constitution.

The petition argues that sub-rule (2) of Rule 3 of the guidelines mandates intermediaries to place restrictions on the kinds of content that a user can post with a broad list of information that is highly subjective and can result in wide interpretation. Additionally, most of these terms are outside the reasonable restrictions provided under Article 19(2) of the constitution. The impugned rules result in the removal of any content that is disliked by any person or is not in his/her interest. The rules empower private parties to censor content over the Internet and places on them the burden to decide the lawfulness of the content, which should normally be a judicial function. The decision to take down content does not provide any opportunity to the owner of content to appeal, nor is the person informed.

D. Peoples' Union for Civil Liberties[230]

Peoples' Union for Civil Liberties, a human rights organization has filed a writ petition in the Supreme Court of India arguing that Section 66A of the Information Technology Act, 2000, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 and the Information Technology (Intermediaries guidelines) Rules, 2011 are in violation of Articles 14, 19, and 21 of the Indian Constitution.

1. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

The petition makes a number of arguments while arguing that the 2009 rules violate the Constitution. It argues that the rules do not offer the creator or author of the content a reasonable opportunity to be heard before blocking the content. The creator is not even informed about the content being blocked. There is no provision for a post decision hearing, or to appeal the blocking order under the rules. Additionally, there are no safeguards or guidelines provided, which need to be followed while making a decision.

2. Information Technology (Intermediaries guidelines) Rules, 2011

The petition argues that none of the terms under rule 3(2) of the intermediary rules are defined, and most of these terms are incompatible with Article 19(2). The rules are vague and ambiguous and do not provide the user reasonable opportunity to know what is permitted so that he/she may act according to law. The rules empower private entities to censor content over the Internet and place on them the burden to decide the lawfulness of the content without any legislative guidance, thereby forcing an adjudicatory role on an intermediary. The decision to take down

[229] Mouthshut.Com (India) Pvt. Ltd. & Anr. v. U.O.I. & Ors., W.P. (C) No. 217 (2013) (India), *available at* http://www.mouthshut.com/pdf/main_pitition.pdf.
[230] Peoples Union for Civil Liberties v. U.O.I. & Ors., W.P. (Crl.) No. 199 (2013) (India), *available* at https://drive.google.com/a/nludelhi.ac.in/file/d/0B_-V5K_jBhEXcmd1SmdVVFFGNDQ/edit.

content is made by the intermediary without hearing the party whose content is affected and without even notifying them of the removal.

Under these rules, similar content is treated differently across online and offline spaces. The rules also state that the intermediary has to take action upon a complaint by any affected person, however, who qualifies as an "affected person" has not be defined anywhere.

The petition also argues that the intermediary rules are ultra vires the parent statute as the guidelines formed under section 79 of the IT Act can only be related to 'due diligence' and the rules in their current form go a step further and legislate on various issues, including the information that can be posted online by a user, whereas the parent provision does not intend any prohibition.

E. Internet and Mobile Association of India231

Internet and Mobile Association of India, an industry body representing Internet platforms and businesses, has filed a writ petition in the Supreme Court of India arguing that Section 79(3)(b) of the Information Technology Act, 2000 is inconsistent with Articles 14 and 19 of the Constitution, and that the Information Technology (Intermediaries guidelines) Rules, 2011 are in violation of Articles 14, 19, and 21 of the Indian Constitution.

The petition states that the peremptory obligation on intermediaries under Section 79(3)(b) to disable or take down content is in violation of Articles 14 and 19 of the Constitution of India. According to the petition, Section 79(3)(b) deprives intermediaries of access to judicial recourse before removing material since intermediaries are required to take down unlawful material upon being notified by a private party or the Government. This violates the freedom of expression of the users and has a chilling effect on speech.

1. Information Technology (Intermediaries guidelines) Rules, 2011

The petition argues that the terms under rule 3(2) of the intermediary rules are vague and ambiguous and do not provide the user with reasonable opportunity to ascertain what is lawful content he/she may conform with the law. The petition also states that Rule 3(2)(b) is ultra vires Section 79(3)(b) of the IT Act since the rule goes beyond the legislative mandate of requiring intermediaries to disable content which is 'unlawful' and creates new categories of substantive ban. With respect to Rule 3(2)(f), the petition takes the view that it is ultra vires since it goes beyond the legislative mandate of requiring intermediaries to disable content that is 'unlawful'. It argues that this rule creates new categories of substantive proscriptions of speech that are not defined anywhere in Indian law.

The petition also argues that Rule 3(4) of the Intermediary Guidelines is in conflict with Section 79(3)(b), which requires an intermediary to act when allegedly unlawful information is brought to the "actual knowledge" of the intermediary. Rule 3(4) exceeds the limits of Section 79(3)(b) by making reference to the intermediary "obtaining knowledge by itself." The petition says that this language implies pro-active monitoring by an intermediary although Section 79(3)(b) of the IT Act does not obligate intermediaries to pro-actively monitor data/information unless it is

[231] Internet and Mobile Association of India & Anr. v. U.O.I. & Anr., W.P. (C) No. 758 (2014) (India), *available at* https://drive.google.com/a/nludelhi.ac.in/file/d/0B3Do3-9ZtwCrNnQzQTg5QmJFRjA/view.

brought to their attention by a third party or the Government. This rule is therefore seen as going beyond the scope of the parent provision and as an unreasonable requirement that is practically impossible to comply with given the volumes of data handled by intermediaries. Finally, the petition states that Rule 3(7) has the effect of circumventing the limitation placed on the State's power by Article 21 of the Constitution.

F. Kamlesh Vaswani[232]

Kamlesh Vaswani, an Indian advocate has filed a petition before the Indian Supreme Court, which seeks to declare sections 66, 67, 69, 71, 72, 75, 79, 80 and 85 of the Information Technology Act, 2000 as unconstitutional. It also asks the Government to frame a specific law and a national policy on pornography, to make viewing pornography an offence, and to direct intermediaries to proactively monitor and block all pornographic content on the Internet.

G. Sabu Mathew George

Sabu Mathew George,[233] a member of the National Inspection and Monitoring Committee constituted under the Pre-Conception and Pre-Natal Diagnostic Techniques (PCPNDT) Act, 1994, and his Non Governmental Organisation co-petitioner, Voluntary Health Association of Punjab, have filed a petition before the Supreme Court of India. The petition states that, the provisions of the PCPNDT Act, are being violated by various search engines as advertisements related to sex determination techniques and products are being displayed in India by these search engines.[234] It further asks that the Department of Electronics and Information Technology at the Ministry of Communications and Information Technology and the competent authority of Department of Health and Family Welfare work harmoniously to implement the provisions of the Act.[235] The petition is not publicly available and it is possible that it seeks other remedies that have not been reported in the media.

---

[232] Kamlesh Vaswani v. U.O.I & Ors., W.P. (C) 177 (2013), *available at* https://docs.google.com/a/nludelhi.ac.in/document/d/1ZyBevXbdC-FXzkSNA9itU5oFjhwO7CNSmZ7_H0Ji_B0/edit.

[233] Sabu Mathew George v. Union of India, W.P. (C) No. 341 (2008) (India)

[234] Shreeja Sen, *Nothing contrary to Indian laws should be advertised online: SC*, MINT (Dec. 5, 2014), http://www.livemint.com/Politics/5fGedpkVoAlvMQHd6nEopL/Nothing-contrary-to-Indian-laws-should-be-advertised-online.html.

[235] Sabu Mathew George v. Union of India, W.P. (C) No. 341/2008, interim order (Dec. 4, 2014), Supreme Court of India (India), *available at* http://supremecourtofindia.nic.in/outtoday/wc34108.pdf.