Eavesdropping on the Freedom of Expression in India

Sunil Abraham[1]

I. Introduction

Today, freedom of expression in India is heavily influenced by policies and practices around intermediary liability and surveillance. Instances like the leaked interceptions in connection with the multi-billion dollar 2G spectrum scam,[2] the National Technical Research Organization's (NTRO) pervasive unauthorized wiretapping of 750,000 phone lines,[3] the 2011 Intermediaries Guidelines Rules, the Cyber Café Guidelines Rules 2011, the Central Monitoring System, and Telecom Minister Kapil Sibal's move to censor Internet content before it is published online,[4] give rise to many important questions about intermediary liability, surveillance, and the freedom of expression in India.

This chapter explores the chilling effect that the Indian government's steps to regulate and monitor Internet content and communications has had on free speech in India. To do this, I examine relevant policies and practices surrounding the freedom of expression and privacy. The research in this chapter

[1] The author thanks Elonnai Hickok for her support.

[2] "Ratan Tata Files Petition in SC on Nira Radia Tapes," *Times of India*, 29 November 2010, http://timesofindia.indiatimes.com/business/india-business/Ratan-Tata-files-petition-in-SC-on-Nira-Radia-tapes/articleshow/7008779.cms.

[3] "Did NTRO Tap Phones?," *Times of India*, 1 August 2011, http://www.timesnow.tv/Did-NTRO-tap-phones/articleshow/4380345.cms.

[4] "Kapil Sibal under Attack: 'We Like Our Freedom and We Shall Have It,'" *Times of India*, 7 December 2011, http://timesofindia.indiatimes.com/tech/social-media/Kapil-Sibal-under-attack-We-like-our-freedom-and-we-shall-have-it/articleshow/11020982.cms.

comes from the results of a 2011 policy sting operation that tested the impact of the Intermediary Liability Rules, an analysis of legislation, and an examination of news reports—as there is scant scholarship and official documentation about Indian security organizations and their affairs. To the extent of the bias in the underlying reporting, that bias might be carried forward here.

In India the freedom of expression is upheld by Article 19 of the Constitution of India as a fundamental right. There are only eight limits on this right: security of the state, friendly relations with foreign states, public order, decency and morality, contempt of court, defamation, incitement to an offence, and protection of the sovereignty and integrity of India.[5] In light of the growing use and widespread impact of the Internet, provisions impacting freedom of expression have appeared in other legislation and policy related to intermediary liability and surveillance.

II. Intermediary Liability Law and Policy

Law and policy in India regulating intermediaries almost always contains provisions that broadly define speech that is prohibited on the Internet and require intermediaries to (1) monitor, and remove when necessary, content that is put online; (2) retain logs of removed content and user information/browsing history; (3) limit anonymous speech; and (4) allow access to retained content when requested by law enforcement. These requirements negatively impact freedom of expression by limiting speech that is permitted and removing the option of anonymous speech, monitoring/retaining all/unspecified speech, and using it for purposes without the knowledge or consent of the individual.

A. Intermediaries Guidelines Rules 2011

In April 2011 the government of India notified the Intermediaries Guidelines Rules under Section 79 of the Information Technology Act 2000.[6] The Rules mandate that intermediaries implement a Terms of Service (ToS) that describe what content is and is not allowed to be posted, and holds intermediaries liable if they do not act upon take-down notices that bring to their attention content that is in violation of the ToS.

---

[5] The Constitution of India 1949, Article 19(1)(a), http://indiankanoon.org/doc/1142233/.

[6] The Intermediaries Guidelines Rules 2011, http://www.mit.gov.in/sites/upload_files/dit/files/GSR314E_10511%281%29.pdf.

Under the Rules, intermediaries are also required to inform users that in the case of noncompliance, the intermediary has the right to discontinue the access and usage rights of the user, and in addition will remove noncompliant content.[7] The rule lists 30 broad, and often vague, reasons for which content may be considered "noncompliant" and worthy of being removed.[8]

In order to enforce these conditions, the Rules have created a system of private censorship with an embedded monitoring regime, in which affected individuals can issue take-down notices "in writing or through email signed with an electronic signature" to the intermediary. If a notice is served, the intermediary must respond within 36 hours of receiving the notice. Any content removed by the intermediary upon notice and associated logs must be preserved for a period of 90 days for the purposes of investigation.[9] When requested in writing, intermediaries are required to provide any authorized governmental agency with information for the purposes of "verification of identity, prevention, detection, investigation, prosecution, cyber security incidents, and punishment for any law for the time being in force."[10]

In many ways, the Rules go beyond the constitutional limits on free speech in India. This is particularly true because the Rules entrust private intermediaries, usually corporations, with the role of censoring content, while giving any unaffected individual the right to ask for censorship. At the same time, the Rules allow for potential monitoring of content by the government by providing authorized agencies access to removed content through provisions that set a lower standard for access than traditional access provisions in the Criminal Procedure Code. Thus, despite statements from the government that the Rules do not violate freedom of expression, the international and national press have criticized the provisions for encouraging the abuse of

---

[7] Ibid., Sec. 3(5).

[8] This includes: "information that belongs to another person and to which the user does not have any right to, is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever, harm minors in any way, infringes any patent, trademark, copyright or other proprietary rights, violates any law for the time being in force, deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature, impersonate another person, contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource, threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting to any other nation" (Intermediary Liability Rules 2011, Sec. 3(2)(a-i)).

[9] Ibid., Sec. 3(4).

[10] Ibid., Sec. 3(7).

take-down notices and summary removal of content without adherence to the principles of natural justice.[11]

B. Cyber Café Guidelines 2011

In addition to the Intermediaries Guidelines, in 2011 the Indian government notified the Guidelines for Cyber Cafés under the Information Technology Act 2000 (ITA).[12] Among other things, these Guidelines require cyber cafés to maintain the following records for at least one year:

1. A scanned or photocopy record of user identification documents.[13]
2. A log register containing the name, address, gender, contact number, type and detail of identification document, date, computer terminal identification, log in time, and log out time.[14] The log register should also contain date-wise details on the usage of a computer resource.[15]
3. Log records for each access or login by any user of the history of websites accessed and the logs of proxy servers installed at cyber cafés.[16]

These records, along with any document, register, or other necessary information must be provided to an officer authorized by the registration agency for cyber cafes.[17] In effect, these requirements take away cyber café user's ability to browse anonymously without having their online activity monitored, stored, and retained.

C. Registration of .in Domain Names and Know Your Customer (KYC) Requirements

An individual's ability to use the Internet anonymously is also limited by the requirements for registration of a .in domain name. Unlike many country

---

[11] For example, see R. Baily, "Censoring the Internet: The New Intermediary Guidelines," *Economic Political Weekly*, 4 February 2012, http://www.indianet.nl/pdf/epw120204.pdf; H. Timmons, "India Asks Google, Facebook to Screen User Content," *New York Times*, 5 December 2011, http://india.blogs.nytimes.com/2011/12/05/india-asks-google-facebook-others-to-screen-user-content/.

[12] Guidelines for Cyber Café Rules 2011, http://mit.gov.in/sites/upload_files/dit/files/GSR315E_10511%281%29.pdf.

[13] Ibid., Sec. 4(2).

[14] Ibid., Sec. 5(2).

[15] Ibid., Sec. 5(3).

[16] Ibid., Sec. 5(4).

[17] Ibid., Sec. (7).

domains, .in, which is regulated by the National Internet Exchange, does not allow for anonymous registration. For example, the Terms and Conditions for Registrants require registering individuals to provide contact details including their full name, postal address, email address, voice and telephone number, and fax number.[18] Further limiting anonymous speech, the government of India requires individuals purchasing SIM cards and installing broadband connections to provide full and accurate details of identification.[19] While open and unsecured Wi-Fi is illegal, and individuals using public Wi-Fi in India must verify themselves by either providing a copy of their photo identity, or through login and password via SMS on their phone. In both cases the provider of the public Wi-Fi must store the copy of identity or mobile number for a period of one year.[20]

III. Surveillance Law and Policy

Alongside the policies directly regulating intermediaries, another limiting factor to the freedom of expression in India is the pervasive state surveillance regime deployed by the Indian government. Though state surveillance most directly infringes on an individual's right to privacy, surveillance indirectly impacts the freedom of expression, as it limits an individual's perception that they can express themselves freely. Thus, state surveillance negatively impacts the freedom of expression to the extent that it limits an individual in their ability to, and the security with which they freely share and exchange ideas with others—both in and outside of India.[21]

A. Interception Law

There are two important statutes in India that permit the interception of communications between individuals: the Indian Telegraph Act, 1885 (TA), and the Information Technology Act 2000 (ITA). These statutes reproduce simi-

[18] Terms and Conditions for Registrants, Points 1 and 3, http://www.registry.in/system/files/Terms_and_Conditions_for_Registrants_1.pdf.

[19] Section 41.14, Unified Access Service License, http://www.auspi.in/policies/UASL.pdf.

[20] Department of Telecommunications, Instructions under the Internet Service Licence Regarding Provision of Wi-Fi Internet Service under Delicensed Frequency Band, 23 March 2009, Section I(b)(ii), http://www.dot.gov.in/sites/default/files/Wi-%20fi%20Direction%20to%20ISP%2023%20Feb%2009_5.pdf.

[21] In the Reporters without Borders report "Internet Enemies 2012: Countries under Surveillance—Eritrea," it was found that the majority of Eritreans reverted to self-censorship because of the surveillance and atmosphere of terror that Dictator Isaias Afewerki had imposed, http://www.unhcr.org/refworld/country,,,ANNUALREPORT,ERI,,4fba1def1b,0.html.

lar restrictions as those applied to the freedom of expression. Under the TA interception is allowed in six circumstances:

1. In the interests of sovereignty
2. Integrity
3. Security
4. Friendly relations with foreign states
5. Public order
6. Preventing incitement to the commission of an offense

These restrictions are allowed to be used under the preconditions that there is a public emergency or in the interest of public safety.[22] Though the ITA replicates the same grounds for interception, it also allows for interception in two additional circumstances[23]—for preventing the incitement to the commission of any cognizable offence relating to the above to for investigation of any offence. Additionally, the ITA, unlike the TA, does not require that public emergency or public safety be preconditions for interception.[24]

Though the right to privacy, unlike the freedom of expression, is not explicitly guaranteed by the Constitution of India, the courts in India have consistently read this right into the fundamental right to life and personal liberty,[25] specifically in the context of interception. For example, in *PUCL* v. *Union of India*[26] the Honorable Court maintained that interception is an infraction of the constitutionally guaranteed right to life and personal liberty unless it is authorized by the legally established procedure established. As directed by the Honorable Court, on 1 March 2007, the central government issued procedural safeguards for interception as rules under the TA.[27] Among other things, the Rules established: the Secretary to the Government of India in the Ministry of Home Affairs and the Secretary to the State Government of the Home Department as the competent authorities

[22] Telegraph Act, 1885, Section 5(2).

[23] "For preventing the incitement to the commission of any cognizable offence relating to the above or for investigation of any offence."

[24] Information Technology Act, 2000, Section 69.

[25] *R. Rajagopal* v. *State of T.N*, http://indiankanoon.org/doc/501107/; and summarized in *Naz Foundation* v. *Government of Delhi*, W.P. (C) No. 7455/2001 (2009), http://www.nazindia.org/judgement_377.pdf.

[26] This has been the only case to challenge Section 5(2) of the Telegraph Act (People's Union for Civil Liberties, "PUCL PIL Challenging Validity of a Section in the Telegraph Act, 1885," People's Union for Civil Liberties website, December 2008, http://www.pucl.org/Topics/Law/2009/telegraph-act.html).

[27] Ibid., Indian Telegraph Rules, 1951, as most recently amended in 2007 under Rule 419A, http://www.dot.gov.in/Acts/English.pdf.

for approving interception requests,[28] a review committee for ensuring that interception orders are in compliance with the Act,[29] and a chain of custody for interception orders and collected material for both service providers and security agencies.[30]

Under the ITA,[31] Section 69 of the Act governs interception of all information transmitted through any computer resource. In 2009, the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Interception) Rules were notified.[32] These Rules, among other things, allow for the real-time monitoring and interception of messages in transit or in storage,[33] require intermediaries to provide "in house" facilities and assistance for intelligence agencies to conduct monitoring,[34] require decryption key holders to disclose decryption keys[35] and provide decryption assistance, and holds intermediaries liable to both imprisonment and fine for noncompliance.[36] Also in 2009 under Section 69B of the ITA, the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules were notified. These Rules enable the government to collect and monitor traffic data upon direction from the Secretary to the government of India in the Department of Information Technology for the protection of cyber security, identification, and prevention of the spread of computer viruses.[37]

Stored information (data at rest) held by service providers can also be accessed via Sections 91 and 92 of the Code of Criminal Procedure (CrPc). If access is sought through Section 91 of the CrPc, an order from an officer in charge of a police station is needed. If access is sought through Section 92, a magistrate, executive or judicial, or any Commissioner of Police, or District

---

28 Section 2(1).
29 Section 2(17).
30 Section 2(7–15).
31 The Information Technology Act 2008, http://www.cyberlaws.net/itamendments/IT%20ACT%20AMENDMENTS.PDF.
32 "Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Interception) Rules Interception, Monitoring, and Decryption Rules," http://bsu.bih.nic.in/%28S%280yao2aqcn3lpmoytiterkk55%29%29/static/downloads/itact/it-procedure-interception-monitoring-decryption-rules-2009.pdf.
33 Ibid., Sec. 4.
34 Ibid., Sec. 13.
35 Ibid., Sec. 17.
36 Ibid., Sec. 25(5).
37 "Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009," http://cis-india.org/internet-governance/resources/it-procedure-and-safeguard-for-monitoring-and-collecting-traffic-data-or-information-rules-2009.

Superintendent can pass an initial order for access, but a court order is needed for further investigation.[38]

B. Interception Policy

In India, the Internet Services License Agreement and the Unified Access Services Licence Agreement, which are established under the Indian Telegraph Act, 1885, govern the activities of telecommunication operators and Internet service providers (ISPs).[39] According to the agreements, the government is afforded extensive access to communication data held by ISPs. For example, the government has the right to inspect/monitor any system of the service provider, and to require service providers to install specific equipment on their networks. Service providers are also responsible for the provision of interception facilities, and must provide location data and CDRs when requested. Furthermore, service providers must make available a list of all subscribers to its services on a password-protected website for easy access by government authorities. The licenses also specify that service providers cannot employ bulk encryption or encryption over 40 bits.[40] In light of these expansive powers, it is important to note that because the ISP agreements refer back to the provisions of the Telegraph Act, the powers found under the license technically cannot legally be wider than the powers granted under the Act itself.

Broadly, when compared with international policies, both the policy/legislation regulating intermediaries and the policy/legislation surrounding state surveillance lack critical safeguards such as: transparency of procedure, notification, redress, and judicial oversight. These gaps in the Indian regime have resulted in the implementation of policy without adequate legislative and judicial checks, thus allowing the government significant rights to curtail free speech.

IV. Chilling Effects of Intermediary Liability Policy

A. Governmental Content Removal Requests

In India there is little transparency as to the extent and scale of government-initiated surveillance and censorship by the government, thus the extent of

[38] The Code of Criminal Procedure, 1973, Sections 91 and 92, http://www.vakilno1.com/bareacts/CrPc/s91.htm.

[39] License Agreement for Internet Services, http://www.dot.gov.in/isp/Internet-licence-dated%2016-10-2007.pdf; Unified Access Service License, http://www.auspi.in/policies/UASL.pdf.

[40] Ibid ISP License, Sec. 2.2, Sec. 30-35; UASL License: Sec. 32, Sec. 37–42.

these activities via intermediaries is unclear. One data point that brings some light to the issue is the Google Transparency Report. According to the report, over a span of six months in 2011, there were 68 governmental requests for content removal and 360 requests for items to be removed. Of these, 51% of requests were fully or partially complied with.[41] In India the trend for removal requests and subsequent compliance has been increasing. For example, in comparison with 2011, in 2010 the government issued 67 content removal requests and 282 item removal requests. Of these, 22% were fully or partially complied with.[42] Between July and December 2012 the total number of content removal requests was 2,944.[43] The 2013 Google Transparency Report also stated "The number of content removal requests we received increased by 90% compared to the previous reporting period."[44]

B. Chilling Effects on Free Expression on the Internet Report

In order to gain a clearer picture of how censorship happens through intermediaries, in the summer of 2011, Rishabh Dara, a Google Fellow with the Centre for Internet & Society, conducted a study with the objective of determining whether the criteria, procedure, and safeguards of the Rules impacted free expression. The study demonstrates that the Rules have had a chilling effect on the freedom of expression in India.[45] Furthermore, the study shows that the poorly designed intermediary liability provision had the following shortcomings: insufficient immunity for the intermediary (for example, treating a multinational corporation and an individual blogger similarly), unconstitutional limits on free speech, the use of undefined and unclear terminology, the lack safeguards and penalties to prevent abuse of the take-down system, lack of transparency (the general public is not informed and nor is the person being censored), and no clear procedure of redress for those wrongfully censored.[46]

During the study, take-down notices were issued to seven different intermediaries. Of the seven, six intermediaries removed content that was

---

[41] Google Transparency Report, Removal Requests, 2011, http://www.google.com/transparencyreport/removals/government/IN/?p=2011-06.

[42] Google Transparency Report, Removal Requests, 2010, http://www.google.com/transparencyreport/removals/government/IN/?p=2011-06.

[43] Google Transparency Report: Break Down by Reporting Period Table, http://www.google.com/transparencyreport/removals/government/IN/.

[44] Google Transparency Report, http://www.google.com/transparencyreport/removals/government.

[45] Rishabh Dara, "Intermediary Liability in India: Chilling Effects on Free Expression on the Internet," The Centre for Internet & Society, 2012, http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf.

[46] Ibid., Executive Summary.

both specified and nonspecified in the take-down notice. The only take-down notice that was not complied with was one sent to an intermediary (Intermediary F in the report), an online shopping portal which provides a platform for buyers and sellers to connect with each other. The take-down notice was sent without supporting evidence and targeted the sale of a particular brand of baby diapers with the statement that:

> such diapers cause Irritant Diaper Dermatitis (commonly referred to as baby rashes) on the convex surfaces of the minor (commonly referred to as the baby's butt) when the skin is exposed to prolonged wetness, increased skin pH caused by urine and feces (commonly referred to as baby's poop).[47]

The take-down notice argued that because of this, the information "harmed minors" as prohibited under Rule 3(2)(c). The intermediary responded to the take-down notice by calling it frivolous, and threatened to take legal action if the take-down notice was not withdrawn.[48] Though it was encouraging that the intermediary recognized the take-down notice as frivolous, this example highlights the fact that the poorly worded provision makes it impossible for the intermediary to take concrete action against fraudulent take-down notices, as the provision does not make it clear what legal action is available for the intermediary to take.

In another example, a take-down notice was sent to an intermediary (Intermediary B in the Report) who hosts news items and allows for commenting. One of the many comments was in response to the Telangana movement and stated:

> Telangana cause is justified, no one is denying that. But have you come to the point, you want to burn India? This is what I am opposing, burning demolition, killing etc. Is the hidden agenda of vested Interests. And we Hyderbadis (Hindues and Muslimes) [sic] will not allow any one to burn our homeland.[49]

A take-down notice was served to the intermediary, stating, among other things, that the comments were "racially and ethnically objectionable," "hateful," "disparaging," and "defamatory" as prohibited under Rule 3(2)(b). The intermediary responded by taking down the comment pointed out in the notice, along with 15 other comments published below the news article.[50]

---

47 Ibid., Sec. 3.6.2, 25.
48 Ibid., Sec. 3.6.3, 26.
49 Ibid., Sec. 3.2.2, 13.
50 Ibid., Sec. 3.2.3, 14.

In yet another example a take-down notice was issued to an intermediary (Intermediary A in the Report), which was an information-location tool, specifically a search engine. The notice asked for "the removal and disablement of three communication link provided in its search engine results on searching for the keywords 'online gambling,'" as prohibited under Rule 3(2)(b). The notice asked the intermediary to

> confirm by email or writing within 36 hours that (i) it has removed the impugned communication links; . . . (ii) it will refrain from, and also prevent it's [sic] users from, hosting, displaying, uploading, modifying, publishing, transmitting, updating, or sharing any similar communication link; . . . (iii) it has terminated the user accounts from which such communication links were hosted, displayed, uploaded, modified, published, transmitted, updated or shared.

The intermediary responded in 120 hours and claimed that "the take-down regime is not applicable to search engines as they fall within the scope of the exemption offered by Rule 3(3)proviso(a)."[51] Despite this, the intermediary still removed the three communication links and all other URLS for the three links, including subdomains.[52]

Similarly, a take-down notice was sent to an intermediary (Intermediary D in the Report) that was a host and an information location tool that provided multiple services, including news, shopping, etc. The take-down notice asked for the "removal and disablement" of three communications links that related to "online gambling" as prohibited under Rule 3(2)(b).[53] In response, the intermediary rejected the notice because the author had not established himself as an affected party, and claimed exemption under Rule 3(3) proviso(a). Despite rejecting the notice, the intermediary took down the three communication links along with all other URLS to the three websites, including subdomains.[54]

---

[51] Section 3(3)proviso(a) of the Rules states: "The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified . . . provided that the following actions by an intermediary shall not amount to hosting, publishing, editing, or storing of any such information as specified in sub-rule (2): (a) temporary or transient or intermediate storage of information automatically within the computer resource as an intrinsic feature of such computer resource, involving no exercise of any human editorial control, for onward transmission or communication to another computer resource."

[52] Ibid., Sec. 3.1, 7.

[53] Ibid., Sec. 3.4.2, 18.

[54] Ibid.,. Sec. 3.4.3, 18.

In conclusion, the study found that the vague language in the Rules causes uncertainty in the criteria and procedure that intermediaries must follow for determining what content to remove, thus leading to a situation where intermediaries are more likely to comply with take-down notices than not. The study highlights that for freedom of expression to be protected there is a need to (1) establish safeguards to prevent the misuse of the take-down regime; (2) clearly establish a procedure for the take-down process; (3) put in place mechanisms to ensure transparency and natural justice in the take-down process; and (4) create a standard test for intermediaries to determine what content should and should not be removed from websites.[55]

In August 2012, a round table discussion was arranged by Telecom Minister Kapil Sibal, Secretary of the Department of Information Technology J. Satyanarayana, and National Cyber Security Coordinator and Director General of CERT-in Dr. Gulshan Rai. The meeting was meant to address the many concerns regarding the Intermediary Guideline Rules and to, as stated by Kapil Sibal in the news item, "tweak these rules in such a way that they are acceptable to everybody." At the meeting private sector companies and organizations, such as Yahoo!, the National Association of Software and Services Companies (NASSCOM), and the Indian Cyber Café Association, critiqued the Rules for placing the burden of determining what content should and should not be removed by intermediaries, creating due diligence procedures that were too strict to be realistically complied with, and for using overly broad language (such as "blasphemous," "defamatory," "ethnically objectionable," etc.).[56]

C. Court Cases Concerning Intermediary Liability

Coinciding with the conclusion of Rishabh Dara's study in September 2011, Kapil Sibal publicly asked social media sites to proactively screen out inflammatory and disparaging content. According to Sibal, even if a company's servers exist outside of India, they still need to be subject to domestic law, and cannot violate Indian statutes.[57] Sibal asked Facebook, Google, Twitter and others to put in place an arrangement where content is screened before going online.[58] Following this request, a criminal complaint and a civil suit was filed

[55] Ibid.; Dara, "Intermediary Liability in India."

[56] S. Singh, "Stakeholders Steadfast on Changes in IT Rules," *The Hindu*, 3 August 2012, http://www.thehindu.com/news/national/article3718615.ece.

[57] Timmons, "India Asks Google, Facebook to Screen User Content"; "Social Media Too Needs Regulations: Kapil Sibal," *IBN Live*, 24 February 2012, http://ibnlive.in.com/news/social-media-too-needs-regulations-kapil-sibal/233335-3.html.

[58] "Online Uproar as Kapil Sibal Seeks Social Media Screening," *Times of India*, 6 December 2011, http://timesofindia.indiatimes.com/tech/news/Internet/Online-uproar-as-Kapil-Sibal-seeks-social-media-screening/articleshow/11006585.cms.

against Google, Facebook, and 18 other Internet intermediaries by two individuals in separate cases. The criminal case asked for content alleged to be hate speech and obscene material to be removed.[59] The civil case asked for content alleged to be defamatory, derogatory, and per se inflammatory to be removed.[60] The cases are going on at the magistrate courts in Delhi with a quashing appeal by the intermediaries also simultaneously being heard by the High Court.[61] In the criminal case, the Lower Court removed several of the accused websites as the registered addresses were not available. In response to the appeal filed in the High Court, the proceedings against Microsoft were quashed. The cases are currently subjudice. Based on news coverage of the trials and statements made by politicians it is clear that the Union Government of India is pushing for the take down of content, and for a proactive monitoring regime.

The Intermediary Liability Rules, the increasing number of governmental content removal requests, and the Indian government's push for proactive screening of online content all point to growing intolerance of free speech online.

V. Chilling Effects of Surveillance

A. Eavesdropping Agencies

According to the 1996 *PUCL* ruling, there are 5 central agencies as well as the intelligence agencies authorized by the state governments which have been allowed access to request authorization for interception.[62] However, according to news reports there are at least 12 central agencies that have tapped phones

---

[59] Pranesh Prakash, "Section 200 Complaint in *Vinay Rai* v. *Facebook India and Ors*," The Centre for Internet & Society website, 20 February 2012, http://cis-india.org/internet-governance/resources/s200-complaint-vinay-rai-v.-facebook-india-and-ors.

[60] Pranesh Prakash, "*Mufti Aijaz Arshad Qasmi* v. *Facebook and Ors* (Order Dated December 20, 2011)," The Centre for Internet & Society website, 20 February 2012, http://cis-india.org/internet-governance/resources/order-2011-12-20-mufti-aijaz-arshad-qasmi-v-facebook-and-ors.

[61] "Can Block Websites Like China, Delhi High Court Warns Facebook, Google," *NDTV*, 13 January 2012, http://www.ndtv.com/article/india/we-can-block-websites-delhi-high-court-warns-facebook-and-google-166383.

[62] People's Union for Civil Liberties, "PUCL PIL Challenging Validity of a Section in the Telegraph Act, 1885." These include: Director Intelligence Bureau, Director General Narcotics Control Bureau, Revenue Intelligence Bureau and Central Economic Intelligence Bureau, Director Enforcement Directorate.

using authorization.[63] Additionally, state-level agencies, like the police, conduct wiretaps on a regular basis.[64] The number of bodies given interception and/or access powers is continuing to expand, as can be seen by the Reserve Bank of India and the Securities and Exchange Board of India being granted the power to access individual call record details in 2013.[65]

B. Scope and Scale of Surveillance

In India corporations and the government are not legally required to be transparent about the extent and nature of surveillance in which they engage. Despite this, there are a few publicly available data points that reveal the scope of governmental surveillance. In 2010, news items cited the Indian government as admitting to legally tapping over 6,000 telephones in New Delhi per year.[66] To place these numbers in perspective, in 2010, in the United States, 3,194 authorized intercepts were conducted.[67] As another data point, in 2011, Reliance Infocomm filed an affidavit stating that in 2005 the company intercepted 3,588 phones in New Delhi alone, and between 2006 and 2010, the company intercepted 1.51 lakh telephones throughout India at the request

---

[63] Intelligence Bureau, Narcotics Control Bureau, Central Economic Intelligence Bureau, Directorate of Revenue Intelligence, Central Board of Direct Taxes, Research Analysis Wing, Central Bureau of Investigations (Ritu Sarin, "Govt Sets Norms for Lawful Interception and Monitoring," *The Indian Express*, 17 February 2012, http://www.indianexpress.com/news/govt-sets-norms-for-lawful-interception-and-monitoring/913034/0); Income Tax Department ("SC Directs IT Dept to Transcribe Tapped Conversation of Radia," DNA, 6 September 2012, http://www.dnaindia.com/india/report_sc-directs-it-dept-to-transcribe-tapped-conversation-of-radia_1737582); the National Technical Research Organization ("The Listeners," *The Indian Express*, 6 June 2012, http://www.indianexpress.com/news/the-listeners/958266/0); Directorate of Signal Intelligence (in sensitive areas of the country), TERM, and DoT (M. A. Arun, "Big Brother, Smaller Siblings Watching You," *The Deccan Herald*, 4 September 2010, http://www.deccanherald.com/content/94085/beware-big-brother-smaller-siblings.html).

[64] A. E. Suresh, "Govt to Come Down Hard on Unauthorized Phone Taps," *Live Mint*, 18 May 2011, http://www.livemint.com/2011/05/18002647/Govt-to-come-down-hard-on-unau.html.

[65] B. Jain, "Govt Gives Sebi, RBI, Access to Call Data Records," *Times of India*, 14 June 2013, http://articles.timesofindia.indiatimes.com/2013-06-14/india/39975284_1_home-ministry-access-call-data-records-home-secretary.

[66] "The Secret World of Phone Tapping," *India Today*, 20 December 2010, http://indiatoday.intoday.in/story/the-secret-world-of-phone-tapping/1/122693.html.

[67] Director of the Administrative Office of the United States Courts, "Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications," June 2011, 5, http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2010/2010WireTapReport.pdf.

of security agencies.[68] Corporate transparency reports are another indicator of the scope of surveillance in India. For example, Facebook's Governmental Requests Report shows that India issued 3,245 data requests in the first six months of 2013,[69] while the Google Transparency Report indicates that in 2011 the government of India made 18,257 user data requests, in the beginning of 2012 it shows that 20,938 user data requests were issued, and by the end of 2012, the GOI had issued 21,389 user data requests.[70] Yahoo, on the other hand, received 1,490 data requests and 2,704 requests on specified accounts in the first six months of 2013.[71]

Despite these numbers, even a high-level understanding of the scope and scale of surveillance in India is not easy as the amount of unauthorized or illegal surveillance that takes place is unknown. It is clear though that "easy to use" technologies with interception capabilities like "off the air" GSM/CDMA monitoring systems, along with a pervasive fear of terrorism, the need to strengthen national and cyber security, and the lack of strong enforcement, has enabled an environment in which legal safeguards and procedures for surveillance can be bypassed. For example, in 2013 it was found in Himachal Pradesh that phones were being intercepted on grounds not defined in the Indian Telegraph Act, 1885, and without proper authorization. It was also found that the intercepted data was being retained longer than the permitted period, and action was not being taken off of collected data.[72] Previously, it was revealed that between 2010 and 2011 a governmental body known as the Defence Intelligence Agency had purchased surveillance equipment without authorization, and despite the issue being brought to the attention of the Prime Minister's Office, the agency was not stopped from using the equipment.[73]

Unauthorized interception can also take place through informal requests from security agencies or law enforcement. News items indicate that these informal requests are regularly issued to service providers, who in turn,

---

[68] "Phone Tapping Has Checks and Balances in Place, Says Govt," *The Economic Times*, 16 February 2011, http://articles.economictimes.indiatimes.com/2011-02-16/news/28552149_1_phone-tap-orders-interception-indian-telegraph-act.

[69] Facebook, Governmental Requests Report, 2013, https://www.facebook.com/about/government_requests.

[70] Google, Transparency Report, http://www.google.com/transparencyreport/userdatarequests/.

[71] Yahoo, Transparency Report, http://info.yahoo.com/transparency-report/.

[72] "Probe into Humachal Phone Tapping Over, Report Submitted," *Znews*, 15 June 2013, http://zeenews.india.com/news/himachal-pradesh/probe-into-himachal-phone-tapping-over-report-submitted_855298.html.

[73] S. Datta and P. Sagar, "DNA Exclusive: PMO Know You Were Being Snooped Upon," *DNA*, 17 September 2012, http://www.dnaindia.com/india/report_dna-exclusive-pmo-knew-you-were-being-snooped-upon_1741818.

more often than not, comply with the requests [74] The probability of informal requests being complied with is augmented by the fact that the Indian surveillance regime does not provide a legal mechanism for service providers to easily challenge requests, and issues a heavy penalty on service providers for noncompliance.[75] In 2013, in an attempt to curtail illegal intercepts from taking place, the Department of Telecommunications proposed a Rs. 2 crore penalty to be added to the interception provisions in the Indian Telegraph Act, 1885.[76]

C. Surveillance Systems

To expand the interception capabilities of security agencies, India has steadily been putting in place infrastructure that allows for electronic monitoring to be carried out on a greater scale and with more granularity. For example, in 2010, the National Intelligence Grid (NATGRID) was established as an attached office of the Ministry of Home Affairs, and is expected to be legalized through an executive order in 2013. The system will significantly broaden the scope of access available to security agencies by linking 21 databases together in real time.[77] Presently, the government is implementing the Centralized Monitoring System (CMS) to enable legal interception in real time in such a way that bypasses the service provider.[78] The government has also made plans to create the National Cyber Coordination Centre for monitoring all traffic coming in and out of the country.[79]

Despite the development and high expectations of these systems, many have been unsuccessful due to high costs, technology failures, and legal provisions that do not allow the government to bypass existing procedure and easily put in place ubiquitous real-time monitoring and interception sys-

---

[74] Arun, "Big Brother, Smaller Siblings Watching You."

[75] Under Section 69 of the Information Technology Act 2000 service providers can be penalized with up to seven years in jail for noncompliance.

[76] "DoT Proposed Rs. 2 Cr. Penalty on Illegal Phone Tapping," *Live Mint & the Wall Street Journal*, 31 May 2013, http://www.livemint.com/Industry/FGyRtuGFdGITuqpXdaT2GI/DoT-proposes-Rs-2-cr-penalty-on-illegal-phone-tapping.html.

[77] A. Sharma, "NATGRID to Get Legal Powers Soon," *The Economic Times*, 10 September 2013, http://articles.economictimes.indiatimes.com/2013-09-10/news/41938113_1_executive-order-national-intelligence-grid-databases.

[78] "Soon Security Agencies to Intercept Email, Chats in Real Time," *Times of India*, 12 May 2011, http://articles.timesofindia.indiatimes.com/2011-05-12/india/29535755_1_security-agencies-cms-intercept.

[79] "Govt Proposes Agency to Monitor Internet Traffic," *Times of India*, 5 March 2012, http://articles.timesofindia.indiatimes.com/2012-03-05/security/31123879_1_cyber-security-nscs-high-level-meeting.

tems. For example, the National Technical Research Organization (NTRO) "Vishwarupal" spy system, which was proposed as part of the CMS system, failed to capture 100% of Internet data, collecting only 3 GBPS of traffic out of 28 GBPS, and crashed multiple times during trial runs.[80] Though the NATGRID first began in 2010, it is only in 2013 that an executive order is being issued to legalize the linking and real-time access of the multiple databases. Similarly, international and national press has repeatedly questioned the legality and transparency of the CMS.[81]

The pervasive nature of these systems without adequate legal safeguards in place, and combined with the trend toward digitizing, recording, and data basing all transactions through schemes like the Unique Identification project (a proposed national identification scheme based on biometrics that is to be adopted by multiple platforms),[82] is facilitating the monitoring and tracking of Indian citizens and residents, without their knowledge across devices, networks, and databases.

In addition to the government developing solutions for interception via independent projects and systems, the Indian government ensures access to individuals' communications and Internet use via technologically requirements for ISPs. In 2012, the government requested that ISPs put in place Lawful Intercept and Monitoring (LIM) facilities so that security agencies would have full access to all services, including BlackBerry Messenger (BBM), Nokia, Pushmail, Skype, Yahoo, Gmail, etc., and included this as a part of the license agreement with the ISPs.[83] Since that time ISPs across India have been seeking approval from the Department of Telecommunications for installed LIM solutions for different services.[84]

---

[80] "Govt's Internet Spy Systems Fail to Capture 100% Data Traffic," *Times of India*, 10 March 2012, http://timesofindia.indiatimes.com/tech/enterprise-it/security/Govts-Internet-spy-systems-fail-to-capture-100-data-traffic/articleshow/12208491.cms.

[81] For example, see P. Duggal, "Central Monitoring System—A Legal Viewpoint," *Deccan Herald*, 20 June 2013, http://www.deccanherald.com/content/341759/central-monitoring-system-legal-viewpoint.html; Human Rights Watch, "India: New Monitoring System Threatens Rights," 7 June 2013, http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights.

[82] H. Kanakia, "A UID Numbering Scheme," UIIDAI, May 2010, http://uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf.

[83] Government of India Press Information Bureau, "Interception Solutions by Networking Service Providers," 14 March 2012. http://pib.nic.in/newsite/PrintRelease.aspx?relid=80948.

[84] For example, in 2013 Vodafone sought approval of their LIM solution for their Video Conferencing Services ("Vodafone Seeks DoT Nod for Pan-India Video Conferencing," *Times of India*, 10 July 2013, http://articles.timesofindia.indiatimes.com/2013-07-10/telecom/40491452_1_telecom-major-vodafone-security-norms-3g-spectrum).

Currently, the Indian interception regime lacks safeguards that would protect the rights of the individual. For example, individuals cannot seek redress if their communications—offline or online—are illegally intercepted by the government. The impact of this lacunae is exacerbated by the fact that India does not adhere to the "fruit of the poisonous tree" doctrine, and evidence for one crime obtained while investigating another crime, is accepted in Indian courts. One example of this is the Ratan Tata case, where the 2G Scam was uncovered while agencies were tapping for tax fraud.[85] In *Shri Omprakash Housilprasad Yadav* v. *Appellate Officer & Deputy Secretary 2007* the Maharashtra State Information Commission denied the petitioners request to know if his phone had been wiretapped, stating that a person is not entitled to receive information as to whether his telephone has been tapped or not by the government.[86]

The scale and scope along with the pervasive and nontransparent nature of state surveillance, and the lack of redress that is afforded to individuals in India, curtails freedom of expression, as individuals have no protection against inaccurate or illegal accusations and penalties supported by surveilled material.

VI. The Chilling Effect on Freedom of Expression

In India there has been a significant dilution of safeguards across surveillance and intermediary liability provisions. In the case of surveillance, traditional access through the CrPc incorporates judicial oversight at some level, yet interception requires approval only from the executive, while monitoring and collection of traffic data needs only the approval of a bureaucrat. Similarly, governmental take-down orders must be approved by a joint secretary of the central government,[87] whereas individuals can now request the removal of any content found to be in contravention with legally permitted content. These dilutions have made it easier for individuals' communications, particularly online, to be monitored and censored, and in effect have had a chilling effect on free speech. Furthermore, the retention and sharing of personal information that is connected to the content that has been

[85] Press Trust of India, "India Needs Law against Invasion of Privacy: Ratan Tata," *The Economic Times*, 16 February 2011, http://articles.economictimes.indiatimes.com/2011-02-16/news/28551990_1_group-chairman-ratan-tata-niira-radia-conversation-with-corporate-lobbyist.

[86] B. Viju, "Phone Taps Not Covered under RTI," *Times of India*, 4 October 2007, http://articles.timesofindia.indiatimes.com/2007-10-04/india/27978189_1_indian-telegraph-act-phone-taps-rti-act.

[87] These Rules are found under Section 69A of the ITA but are not discussed in this paper.

blocked, removed, or filtered, with law enforcement agencies, has negative implications for privacy.

When looking at past targets of surveillance activities in India, it has been mostly political and business personalities that have been targets of wiretapping.[88] Many of these wiretaps, one way or another, end up being leaked to the public supposedly, among other reasons, to expose various scams. Ironically, the fact that the majority of taps conducted are on politicians themselves is important to note, because it highlights an overlooked element of transparency in India's democracy.

As demonstrated by the manner in which the practice of unauthorized interception is ignored by higher authorities,[89] carried out routinely by security agencies,[90] and undertaken for broad and unspecified targets,[91] the distinguishing features of the Indian policy on interception seems to be subsidiarity and informality. As demonstrated above, the present interception and intermediary regime has made it possible for the government to take down, block, intercept, monitor, and target everyday communications through blanket and targeted monitoring and interception. The negative impact of these actions on an individual's right to free speech and privacy is worsened by the lack of enforcement of existing procedures and safeguards.

The government's demand for monitoring, content regulation, and access to services such as BlackBerry, Twitter, and Google curtail the freedom of expression through the threat of content removal and unlimited interception at all costs. From the policy and practice surrounding these regimes, it appears that the Indian government believes that the only way of addressing national threats is through enacting legislation that lack critical judicial/legislative safeguards and severely curtails the freedom of expression, even without proof that such curtailment is effective. By imposing restrictions on the freedom of expression by intercepting communications and regulating online content, both of which authorization for lie outside of the purview of the judiciary, the government seems to have forgotten their responsibility to protect the rights of both the online reader and writer.

---

88 S. Datta, "We the Eavesdropped," *Outlook*, 3 May 2010, http://www.outlookindia.com/article.aspx?265191.

89 This article explains how the Prime Minister's Office and the National Security Advisor turned their heads when it was brought to their attention that the Defense Intelligence Agency was acquiring interception equipment without authorization (Datta and Sagar, "DNA Exclusive").

90 Arun, "Big Brother, Smaller Siblings Watching You."

91 This article describes how Indian security agencies use off the air GSM/CDMA systems in Delhi "in the hope that we might pick up critical conversations" (S. Datta, "A Fox on a Fishing Expedition," *Outlook*, 3 May 2011, http://www.outlookindia.com/article.aspx?265192).

This message can be seen through the media's portrayal of the issues at hand. Recent news items reflect societal perceptions of these new regimes that expand state surveillance. Using phrases such as "Big Brother's Watching You"(*Deccan Herald*),[92] "Phone Tapping: Security Monitoring Body Will Intercept Phone Calls, Analyse Billing Records" (*Economic Times*),[93] "Phone Tapping Serious Assault on Democratic Rights, Says CPI" (*India Today*),[94] "New IT Rules Give Big Brother Free Access to Sensitive Personal Information" (*The Hindu*),[95] and "The Walls Have Ears" (*Outlook*),[96] news items indicate that society does perceive the current regimes having a negative impact on freedom of expression.

When examined simultaneously, both the intermediary liability and the interception regime exemplify how ISPs, online platforms, and telcos are placed in situations where they are forced to comply with the government's orders—resulting in massive infringement on civil liberties. In particular, the right to free speech and the right to privacy.

---

[92] S. Abraham, "Big Brother Is Watching You," *Deccan Herald*, 7 March 2014, http://www.deccanherald.com/content/165420/big-brother-watching-you.html.

[93] J. Philip, "Phone Tapping: Security Monitoring Body Will Intercept Phone Calls, Analyse Billing Records," *Economic Times*, 18 May 2011, http://articles.economictimes.indiatimes.com/2011-05-18/news/29555914_1_communication-security-research-telecom-ministry-cabinet-secretary.

[94] "Phone Tapping Serious Assault on Democratic Rights, Says CPI," *India Today*, 24 April 2010, http://indiatoday.intoday.in/story/Phone+tapping+serious+assault+on+democratic+rights,+says+CPI/1/94445.html.

[95] S. Joshi, "New IT Rules Give Big Brother Free Access to Sensitive Personal Information," *The Hindu*, 10 May 2011, http://www.thehindu.com/sci-tech/technology/article2004533.ece.

[96] S. Datta, "The Walls Have Ears," *Outlook*, 11 July 2011, http://www.outlookindia.com/article.aspx?277470.