THE STATE OF SURVEILLANCE IN INDIA: THE CENTRAL MONITORING SYSTEM'S CHILLING EFFECT ON SELF-EXPRESSION

In June 2013, Edward Snowden shook the world's confidence in personal privacy when he leaked top-secret information about the United States National Security Agency's ("NSA") surveillance program, "Prism."[1] Snowden's leaks shattered the global perception that citizens of the world's leading democracy are free from government intrusion,[2] and it was no surprise that privacy issues took the international stage. At the time of Snowden's leaks, it was little known that, across the globe in India, the largest democracy on the planet had had its own massive surveillance program in the works since 2007[3]—a program that would rival the NSA's. It would enable the Indian government to monitor in real time 900 million mobile and landlines and 160 million Internet users.[4] Interestingly, the scheduled launch of India's surveillance program in April 2013 received little attention from the press;[5] nonetheless, its rollout was timely in light

1. For a detailed discussion of Snowden's leaks and their global implications on privacy, see Angus West, *16 Disturbing Things Snowden Has Taught Us (So Far)*, GLOBALPOST (July 9, 2013, 9:45 AM), http://www.globalpost.com/dispatch/news/politics/130703/edward-snowden-leaks.

2. *See* Zoe Kleinman, *What does Prism tell us about privacy protection?*, BBC NEWS (June 10, 2013), http://www.bbc.co.uk/news/technology-22839609; *Dark Arts, Black Hats*, THE ECONOMIST (July 31, 2013, 11:35 PM), http://www.economist.com/blogs/democracyinamerica/2013/07/surveillance-america-0 ("The steady drip-drop of leaks seems to be wearing down public acceptance of mass snooping.").

3. Official documentation of the program first appeared in the Department of Telecommunications' Annual Report for 2007–2008. DEPARTMENT OF TELECOMMUNICATIONS ANNUAL REPORT (2007–2008), *available at* http://www.dot.gov.in/sites/default/files/English%20annual%20report%202007-08_0.pdf ("The requirements for [the program] have been finalized . . ."). In the Annual Report for 2008–2009, the Department of Telecommunications stated that R&D activities for the project were "ongoing." DEPARTMENT OF TELECOMMUNICATIONS ANNUAL REPORT, *available at* http://www.dot.gov.in/sites/default/files/AR_English_2008-09_0.pdf). The Press Information Bureau publicly announced CMS in a press release on November 26, 2009. Press Release, Press Information Bureau, Centralised System to Monitor Communications, (Nov. 26, 2009), *available at* http://pib.nic.in/newsite/ erelease.aspx?relid=54679.26. It also appeared in the 2012–2017 Report of the Telecom Working Group on the Telecom Sector for the Twelfth Five Year Plan. WORKING GROUP ON THE TELECOM SECTOR FOR THE TWELFTH FIFTH YEAR PLAN REPORT (2012–2017), *available at* http://planningcommission.nic.in/aboutus/committee/ wrkgrp12/cit/wgrep_telecom.pdf ("[the program's] technology caters to the requirements of security management for law enforcement agencies for interception, monitoring, data analysis/mining, anti-social-networking using the country's telecom infrastructure for unlawful activities.").

4. Shalini Singh, *India's Surveillance Project May Be as Lethal as PRISM*, THE HINDU (June 21, 2013, 4:14 PM), http://www.thehindu.com/news/national/indias-surveillance-project-may-be-as-lethal-as-prism/article4834619.ece.

5. Pranesh Prakash, *How Surveillance Works in India*, N.Y. TIMES (July 10, 2013, 2:29 AM), http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/ ("When the government announced that the system . . . commenced in April, the news didn't receive much attention."). *See*

of the global conversation on government surveillance that ensued just two months later.

This Note will attempt to contribute to the growing body of discussion on government surveillance, specifically with regard to India. This Note will explain why India's surveillance program, formally called the Central Monitoring System ("CMS"), poses a severe threat to privacy and democratic free expression. More specifically, this Note will discuss how CMS will prompt a paradigm shift in the way speech is regulated in India from its current system of "private censorship" through telecommunications providers to a system of widespread self-censorship among Indian citizens whose speech is chilled by CMS. Finally, this Note will identify potential barriers to public debate surrounding CMS that will inhibit popular demand for government accountability and reform.

I. INDIA'S CENTRAL MONITORING SYSTEM ("CMS") & THE IT ACT

In order to understand the impending threat to privacy at hand, one must first understand how CMS will operate and what it is capable of. CMS utilizes powerful algorithms that are capable of sifting through data to identify patterns and users in invasive ways.[6] Once fully implemented, CMS will allow the government to "listen and tape phone conversations, read e-mails and text messages, monitor posts on Facebook, Twitter, or LinkedIn, and track searches on Google."[7] Essentially, every form of electronic communication will be under the government's microscope. Even partially written emails saved in draft folders will be vulnerable to government intrusion.[8] CMS will also enable the government to track an individual's movements through the use of location-based GPS monitoring.[9] It will be possible for the government to compile personal dossiers on users with the help of CMS through the collection of personal information that corresponds with target numbers assigned to those users.[10]

---

also Anjani Trivedi, *In India, Prism-like Surveillance Slips Under the Radar*, TIME (June 30, 2013), http://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/.

6. Snehashish Ghosh, *The State is Snooping: Can You Escape?*, THE CENTRE FOR INTERNET & SOCIETY (June 27, 2013), http://cis-india.org/internet-governance/blog/india-together-june-26-2013-snehashish-ghosh-the-state-is-snooping-can-you-escape/.

7. Anurag Kotoky, *India Sets Up Elaborate System to Tap Phone Calls*, REUTERS (June 20, 2013, 2:46 AM), http://www.reuters.com/article/2013/06/20/us-india-surveillance-idUSBRE95J05G20130620.

8. Singh, *supra* note 4.

9. *Id.*

10. *Id.*

Nine government entities—including two spy agencies[11]—will have virtually unfettered access to the sensitive personal information collected through CMS with no court order required to monitor targets,[12] no parliamentary oversight,[13] and no formal privacy regime in place to protect individuals from government intrusion.[14] One expert group created to outline principles for an Indian privacy law described CMS as "an unclear regulatory regime that is nontransparent, prone to misuse, and that does not provide remedy for aggrieved individuals."[15]

The Indian government derives its expansive power to snoop on citizens from the Information Technology Act ("IT Act"). Originally enacted in 2000, and later amended in 2008,[16] the IT Act largely mirrors a law enacted during the colonial era,[17] which permitted the government to

11. The two spy agencies authorized to access surveillance data include the Intelligence Bureau ("IB") and the Research Analysis Wing ("RAW"). The seven other agencies with access include the following: The Central Bureau of Investigation ("CBI"), the Narcotics Control Bureau ("NCB"), DRI, National Intelligence Agency, CBDT (tax authority), Military Intelligence of Assam and JK and Home Ministry. *Id.*

12. Unlike the NSA, which requires court approval to spy on calls or email content, CMS "will work without any independent oversight . . . [T]he agencies can start monitoring targets without the approval of the courts or the parliament." Nandagopal J. Nair, *India's New Surveillance Network Will Make the NSA Green with Envy*, QUARTZ (June 28, 2013), http://qz.com/99019/no-call-email-or-text-will-be-safe-from-indias-surveillance-network/. In commenting on this lack of judicial oversight, Delhi University human rights professor Pawan Sinha remarked that "[b]ypassing courts is really very dangerous and can be easily misused." Kotoky, *supra* note 7.

13. Parliament has played no role in the conception or execution of CMS, and it has never taken any affirmative action to grant the government the power it purports to have in its implementation of CMS. *India: New Monitoring System Threatens Rights*, HUMAN RIGHTS WATCH (June 7, 2013), http://www.hrw.org/news/2013/06/07/india-new-monitoring-system-threatens-rights ("[T]he CMS was created without parliamentary approval."). Talia Ralph & Jason Overdorf, *Is India's Government Becoming Big Brother?*, GLOBALPOST (May 9, 2013, 5:00 AM), http://www.globalpost.com/dispatch/news/regions/asia-pacific/india/120824/india-china-censorship-internet ("[T]his has been done with neither public nor parliamentary dialog.").

14. Bhairav Acharya, *The National Cyber Security Policy: Not a Real Policy*, THE CENTRE FOR INTERNET & SOCIETY (Sept. 25, 2013), *available at* http://cis-india.org/internet-governance/ blog/orfonline-bhairav-acharya-observer-research-foundation-cyber-security-monitor-august-2013-nsp-not-a-real-policy 25, 2013) ("Whereas liberal democracies around the world require such interceptions to be judicially sanctioned, warranted and supported by probable cause, India does not even have a statutory law to regulate such an enterprise.").

15. *India: New Monitoring System Threatens Rights*, *supra* note 13.

16. The earlier IT Act of 2000 made no mention of data interception or decryption as the 2008 amended Act does; it only provided for data decryption. Additionally, the 2008 Act as amended broadens the scope of surveillance to include the investigation of any offense, whether cognizable or not. *Yes, Snooping's Allowed*, THE INDIAN EXPRESS (Feb. 26, 2009), http://www.indianexpress.com/news/yes-snooping-s-allowed/419978/1.

17. The Indian Telegraph Act of 1885 authorizes the government to intercept communications if "it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence." Indian Telegraph Act of 1885, No. 13 of 1885, pt. 2 § 5 INDIA CODE (1993), *available at* http://indiacode.nic.in (amended 2006). Although this Act came into existence at a

intercept communications in the "occurrence of public emergency, or in the interest of the public safety."[18] However, the IT Act "substantially lowers the bar for wiretapping"[19] by removing the requisite preconditions of public emergency or public safety.[20] The IT Act contains several provisions, discussed in later sections of this Note, that grant the central government complete, unfettered discretion to identify targets worthy of surveillance,[21] to mine private data about those targets,[22] and to prosecute them at will.[23] Unsurprisingly, the IT Act raised serious concerns among privacy activists[24] who claim it is repugnant to the Indian Constitution,[25]

---

time when neither cell phones nor the Internet were even contemplated, it still buttresses the operation of CMS today. *See* Adrea Peterson, *India's New Surveillance Program Will Function Under a Law from the Colonial Era*, THINK PROGRESS (July 3, 2013, 9:00 AM), http://thinkprogress.org/justice/2013/07/03/2244361/india-surveillance-colonial-era/.

18. Indian Telegraph Act of 1885, pt.2 § 5.

19. Prakash, *supra* note 5.

20. Like the Indian Telegraph Act of 1885, Section 69 of the IT Act provides for monitoring through data decryption "[i]f the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence." Information Technology Act, No. 21 of 2000, § 69(1), INDIA CODE (1993), *available at* http://indiacode.nic.in. However, missing from the IT Act is the introductory clause "[o]n the occurrence of any public emergency, or in the interest of the public safety . . . ." *See id*.

21. *Id.* § 69.

22. *Id.*

23. *Id*. § 66A.

24. Public anti-CMS groups surfaced in opposition of the implementation of CMS. For example, the #StopICMS campaign (This site has been down for a number of months, so it may be a good idea to replace this group with another that has a more consistent presence on the internet) was an activist blog with an accompanying Twitter account aimed at educating the Indian electorate. *See generally*, http://stopicms.org. Additionally, in June of 2013 the "'Indian wing of the hackers' collective Anonymous announced a multi-city protest against what they termed 'the Indian prism.'" Deepa Karup, *In the Dark About "India's Prism*,*"* THE HINDU (June 16, 2013), http://www.thehindu.com/sci-tech/technology/in-the-dark-about-indias-prism/article4817903.ece.

25. Critics of the law argue that it clashes with Article 21 of the Indian Constitution, which provides that "no person shall be deprived of his life or personal liberty except according to procedure established by law." INDIA CONST. art. 21; *see, e.g.*, Bhairav Acharya, *The Central Monitoring System: Some Questions to be Raised in Parliament*, THE CENTRE FOR INTERNET & SOC'Y (Sept. 19, 2013), http://cis-india.org/internet-governance/blog/central-monitoring-system-questions-to-be-asked-in-parliament; *see also Section 66A of the IT Act Violates the Constitution of India*, THE ECONOMIC TIMES (Dec. 7, 2012), http://articles.economictimes.indiatimes.com/2012-12-07/news/ 35670648_1_section-66a-annoyance-or-inconvenience-reasonable-restrictions ("Clause 2 of Article 19 of the Constitution makes it clear there are "reasonable restrictions on the exercise of the right" granted by subclause A of the Article. The operative word is 'reasonable.'"); Pranesh Prakash, *Practise What You Preach*, THE INDIAN EXPRESS (Apr. 26, 2012), http://www.indianexpress.com/ news/practise-what-you-preach/941491/ ("Section 69 of the IT Act allows the government to force a person to decrypt information, and might clash with Article 20(3) of the Constitution, which provides a right against self-incrimination."). Several public interest suits have been filed challenging the constitutionality of the Act. In one case filed in November 2012, Shreya Singhal submitted to the Supreme Court that Section 66A curbs freedom of speech and expression and violates Articles 14, 19 and 21 of the

inconsistent with Supreme Court precedent,[26] in violation of global privacy standards,[27] and in contravention of international treaties to which India is a party.[28]

Activists are particularly concerned with the government's proclivity to stifle free expression under the IT Act.[29] The discussion that follows will identify two provisions of the IT Act that threaten freedom of expression in India. The first of these provisions, Section 69,[30] curtails speech through "private censorship"[31] by intermediary telecommunications providers. The

---

Constitution. Aparna Viswanathan, *An Unreasonable Restriction*, THE HINDU (Feb. 20, 2013), http://www.thehindu.com/opinion/lead/an-unreasonable-restriction/article4432360.ece.

26. Chinmayi Arun, *Way to Watch*, THE INDIAN EXPRESS (June 26, 2013), http://www.indian express.com/news/way-to-watch/1133737/. In 1996, India's own Supreme Court recognized the need for appropriate procedural safeguards with regard to phone tapping under the *People's Union of Civil Liberties v. Union of India and Another* in order to ensure fairness and reasonableness of surveillance. The court outlined the following procedure for wiretapping:

> I. [T]he order should be issued by the relevant Home Secretary (this power is delegable to a Joint Secretary),
>
> II. the interception must be carried out exactly in terms of the order and not in excess of it,
>
> III. a determination of whether the information could be reasonably secured by other means,
>
> IV. the interception shall cease after sixty (60) day[s].

People's Union of Civil Liberties v. Union of India and Another, A.I.R. 1997 S.C.568 (India). Although some of these safeguards have been accounted for in the IT Act, there is no way for the public to ensure that they are being adequately carried out. *Id.*

27. Arun argues that, when measured against the safeguards for government surveillance recommended by Frank La Rue, United Nations special rapporteur for the promotion of and protection of free speech and expression, the CMS framework is markedly weak in terms of its protections for citizens. *Id.* La Rue's recommendations provide that:

> [I]ndividuals should have the legal right to be notified that they have been subjected to surveillance or that their data has been accessed by the state; states should be transparent about the use and scope of communication surveillance powers, and should release figures about the aggregate surveillance requests, including a break-up by service provider, investigation and purpose; the collection of communications data by the state, must be monitored by an independent authority.

Report Of The Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression, U.N. DOC. A/HRC/23/40 (Apr. 17, 2013).

28. *See India: New Monitoring System Threatens Rights*, *supra* note 13. Article 17 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights provides that, "(1) no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation; (2) everyone has the right to the protection of the law against such interference or attacks." International Covenant on Civil and Political Rights, *opened for signing* Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter "Covenant on Civil and Political Rights"] (entered into force Mar. 23, 1976); Universal Declaration of Human Rights, G.A. Res. 217 (III), art. 17, U.N. Doc. A/810 (1948))) ("(1) Everyone has the right to own property alone as well as in association with others, ((2) No one shall be arbitrarily deprived of his property.").

29. *See infra* Part IV.

30. Information Technology Act, *supra* note 20, § 69.

31. The term "private censorship" is used throughout this Note to describe censorship conducted by private telecommunications companies in India rather than state actors.

second provision, Section 66A,[32] was repeatedly used by the government to prosecute citizens for their expression. The Indian Supreme Court struck down Section 66A on March 24, 2015 declaring the law unconstitutionally vague and prone to arbitrary prosecution of citizens' speech.[33] While the Court's decision eliminated Section 66A's formidable threat to free speech, other Indian laws are still subject to prosecutorial abuse.[34] Furthermore, the history of Section 66A is telling of the government's approach to limiting free speech.

Following the implementation of CMS, India is poised to see a marked shift in the way speech is regulated. The former system of "private censorship" will give way to arbitrary monitoring through CMS and the subsequent prosecution of citizens. This will have a chilling effect on the Indian populace. Ultimately, the implementation of CMS will lead to widespread self-censorship and the suppression of ideas in the marketplace.

II. SECTION 69 & "PRIVATE CENSORSHIP" BY INTERMEDIARY SERVICE PROVIDERS

Section 69 of the IT Act empowered the Indian central government to create a system of "private censorship," whereby the Indian central government monitors and regulates speech through intermediary telecommunications service providers ("ISPs"). Under this system, the government issues orders to ISPs directing them to intercept data, to take down multimedia content, or even to block certain content altogether.[35] Section 69A grants governmental power to direct the blocking of public access to information through any computer resource.[36] Section 69B of the IT Act further provides that the competent authority may "direct any agency . . . to intercept, monitor, or decrypt . . . any information generated, transmitted, received or stored in any computer resource."[37] Should any

32. *Id.* § 66A.

33. Amit Chaturvedi, *"Unconstitutional": Supreme Court Scraps Section 66A, Protects Online Freedom of Speech* (Mar. 24, 2015), available at http://www.ndtv.com/india-news/freedom-of-speech-online-section-66-a-is-struck-down-by-supreme-court-749104. Justices J. Chelameswar and Rohinton F. Nariman declared, "It is clear that Section 66A arbitrarily, excessively and disproportionately invades the right of free speech and upsets the balance between such right and the reasonable restrictions that may be imposed on such right." Jayant Sriram, *SC strikes down 'draconian' Section 66A*, The Hindu (Mar. 25, 2015), http://www.thehindu.com/news/national/supreme-court-strikes-down-section-66-a-of-the-it-act-finds-it-unconstitutional/article7027375.ece.

34. *See infra* note 76 and accompanying text.

35. IT Act §§ 69A, 69B.

36. Information Technology Act, § 69A.

37. *Id.* § 69B.

subscriber, intermediary, or person empowered to intercept the information "fail[] to assist the agency," [S]ection 69 imposes a prison sentence of up to seven years.[38]

Section 79 of the Act reinforces the system of "private censorship" by exposing intermediaries to liability should they refuse to do the government's bidding.[39] Ironically, however, Section 79 is designed to limit intermediary liability. Under this section, an intermediary is immune from liability for third party content made available or hosted by them provided they observe 'due diligence' and follow prescribed norms.[40] In 2011, the Ministry of Communications and Information Technology issued a set of Rules—the Information Technology [Intermediaries Guidelines] Rules, also known as the 2011 IT Rules ("IT Rules"), in order to define and further standardize expectations for intermediaries' compliance with Section 79.[41] However, the 2011 IT Rules missed their mark because they failed to adequately define key terms in the "due diligence" process.[42] For example, Rule 3(2) bars intermediaries from hosting "objectionable," "hateful," "disparaging," and "defamatory"

38. *Id.* § 69. It is suggested that this penalty may well conflict with Article 20(3) of India's Constitution, which provides citizens with a right against self-incrimination. This theory seems plausible in light of the fact that no evidence exists in the public record suggesting that the constitutionality of Section 69 was reviewed. Pranesh Prakash, *Practise What You Preach*, THE INDIAN EXPRESS (Apr. 26, 2012), http://www.indianexpress.com/news/practise-what-you-preach/941491/.

39. Section 79 provides, in part, that intermediaries are not liable so long as they "observe[] due diligence while discharging [their] duties under this Act *and also observe[] such other guidelines as the Central Government may prescribe in this behalf* (emphasis added). Information Technology Act, *supra* note 20, § 79(2)(c).

40. *Id.* This limit on intermediary liability was introduced by the government in the 2008 Amendments to the IT Act. Melody Patry, *India: Digital Freedom Under Threat?*, INDEX ON CENSORSHIP (Nov. 21, 2013), *available at* https://www.indexoncensorship.org/wp-content/uploads/2013/11/india_digital-freedom-under-threat.pdf.

41. Information Technology (Intermediaries Guidelines) Rules, 2011, Gazette of India, pt.Part II, sec.section III (i) (Apr. 11, 2011), *available at* http://deity.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf [hereinafter IT Rules].

41. 2011 IT Rules.

42. Malavika Prasad, *State Regulation of Social Networking Sites: Balancing Sovereignty of States and Free Speech*, GERMAN INST. OF GLOBAL AREA STUD., 6 (2008), http://thegiga.in/LinkClick.aspx?fileticket=dT3TIVzzTx8%3D&tabid=589. Even Parliament has commented on the amorphous language of the IT Rules. *See India: New Monitoring System Threatens Rights*, *supra* note 13:

> In March 2013, a parliamentary standing committee on the 2011 Information Technology rules also noted how vague and ambiguous language such as "grossly harmful," "defamatory," and "obscene" could lead to harassment. It recommended defining terms in the rules to ensure that no new categories of crimes or offenses were created. It also noted that ambiguity in the rules regarding the liability of intermediaries, such as online service providers, encourages them to take down any content that could run afoul of vaguely worded prohibitions to avoid legal penalties.

content.[43] Yet, the Rules do not concretize any of these terms. According to academic Malavika Prasad, this has resulted in "the introduction of an element of subjectivity that renders the whole process vague and ambiguous . . . . Even when intermediaries believe that they may qualify for immunity, the uncertain application of the principles has caused them to err on the side of caution by blocking the content."[44]

What is more, Rule 3(4) requires that the intermediary "disable" infringing content within thirty-six hours of receiving notice of a complaint.[45] Should the intermediary fail to do so, it is subject to criminal prosecution for any allegation flowing from the notice, and the penalty is harsh.[46] This narrow timeframe places a heavy burden on intermediaries to eliminate content without sufficient time to inquire about its legitimacy.[47] The difficulty of complying with the thirty-six hour window is compounded by the fact that ISPs lack both legal expertise and adequate resources to properly address every complaint that they receive.[48] The result is a haphazard, cursory system for reviewing complaints under which legitimate, lawful expression falls through the cracks.[49]

---

43. IT Rules at Rule 3(2).

44. Prasad, *supra* note 42, at 6–7. In 2011, the Centre for Internet and Society ran a series of tests to see how intermediaries responded to illegitimate takedown requests within thirty-six hours. "Of the 7 intermediaries to which takedown notices were sent, 6 intermediaries over-complied with the notices, despite the apparent flaws in them . . . . The results of the [study] clearly demonstrate that the Rules indeed have a chilling effect on free expression." Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet 2011*, CENTRE FOR INTERNET & SOC'Y (Apr. 10, 2012), http://cis-india.org/internet-governance/intermediary-liability-in-india.

45. Privacy Report: India, Privacy International (Nov. 14, 2012), https://www.privacyinternational.org/reports/india-0. In April 2013, the Indian government issued a Clarification on the IT Rules. In it, the government addressed the thirty-six hour window for takedowns, specifying that intermediaries need only respond or acknowledge the complaint within thirty-six hours of receiving it rather than actually removing the content. This did very little to alleviate the brevity of the window for intermediaries to comply with takedown notices. Patry, *supra* note 40 at 6.

46. Section 69A of the IT Act imposes a penalty of imprisonment for up to seven7 years for failing to comply with a takedown notice. Information Technology Act § 69AIT. Interestingly, though,

> [u]nauthorized access to communications data is not punishable per se . . . While there is a provision in the Telegraph Act to punish unlawful interception, it creates a far lesser penalty . . . than for a citizen's failure to assist an agency that wishes to intercept or monitor or decrypt.

Prakash, *supra* note 5.

47. "This narrow timeframe, which does not specifically take into account public holidays or weekends, puts intermediaries in a difficult position where they are required to be overly zealous in taking down content that may be entirely legitimate." Patry, *supra* note 40, at 6.

48. "[I]t can be reasonably presumed that not all intermediaries have sufficient legal competence or resources to deliberate on the legality of an expression." Dara, *supra* note 44, at 2.

49. "This overcompliance [of intermediaries] demonstrates a real chilling effect on freedom of expression, as many intermediaries are overwhelmed with requests or do not have the legal expertise to properly handle them in a manner that protects freedom of expression." Patry, *supra* note 40 at 6.

III. OUT WITH PRIVATE CENSORSHIP, IN WITH CMS

The system of intermediary takedowns, or "private censorship," under Sections 69 and 79 is on its way out with the advent of CMS. Speech will be moderated largely by Indian citizens themselves rather than by ISPs. Fearful of a "Big Brother" government vested with the authority to monitor and prosecute people at will, Indian citizens will begin to self-censor.

In effect, the CMS scheme cuts Indian ISPs from the equation.[50] The CMS infrastructure consolidates the existing "Lawful Interception Systems" installed on the network of all fixed and mobile telecommunications operators, ISPs, and International Long Distance Providers.[51] Furthermore, CMS mandates the installation of additional dedicated interception data servers in each private telecommunications network for surveillance purposes.[52] This creates a kind of central technological nervous system for government intelligence gathering in place of the fragmented, privatized system of the past.

To give this system teeth, the Department of Telecommunications mandates service providers grant the government direct access to the communications they host.[53] In the licenses the Department issues to them, providers are contractually obligated to permit governmental access to information, regardless of whether a warrant exists.[54] Whereas before the government had to request that user information be monitored and turned over to the authorities, under CMS the Indian government can "tap into communications at will without telling the service providers."[55]

---

50. Arun, *supra* note 26. Pre-CMS, the government had to request metadata from the telecommunication firms (e.g. call detail records, visited Web sites, IP address assignments) in order to supply the government with the data it sought. Prakash, *supra* note 5.

51. Singh, *supra* note 4.

52. Aman Sharma, *Govt to Modernise Phone Tapping*, INDIA TIMES (May 6, 2011), http://indiatoday.intoday.in/story/government-plans-to-tighten-phone-tapping-norms/1/137251.html.

53. Prakash, *supra* note 5.

54. *Id.* The director general of the Cellular Operators Association of India commented that, "[w]e are obligated by law to give access to our networks to every legal enforcement agency." Kotoky, *supra* note 7.

55. Kotoky, *supra* note 7. The government reasons that the updated process by which it will obtain information will in fact be more conducive to individual privacy, because it will reduce the risk of leaks and security breaches. Singh, *supra* note 4 ("On November 29, 2009, the government told Parliament that CMS's implementation would overcome 'the existing system's secrecy which can [] easily be compromised due to manual interventions at many stages."). Indian government officials also insist that since "CMS will involve an online system for filing and processing of all lawful interception requests, an electronic audit trail will be in place for each phone number put under surveillance." Nair, *supra* note 12. While the Indian government insists that an audit trail will exist, the officials reviewing

Interception can be authorized in secret within government departments.[56] Power to approve surveillance requests by any of the nine government agencies with authorized access will rest in the hands of the top bureaucrat in the federal interior ministry and his state-level deputies.[57] By eliminating third-party intermediaries, the government will have unfettered access to the communications of any individuals it wishes to target.[58]

India's new surveillance model under CMS raises a host of privacy concerns. With all intermediaries removed and communication interception solely in the hands of government officials, there is a much greater likelihood of "disempower[ing] citizens by relying . . . on the executive to safeguard individuals' . . . rights."[59] One reporter attributed prevailing concerns about privacy in India to "the major technological advancements in monitoring and enhanced forensic capabilities in surveillance, coupled with the change in procedure which mandates the interception authorization to be kept secret between two government departments with no scope of a transparent public disclosure of who is being monitored, for what purpose and for how long, . . ."[60]

Privacy advocates caution against the CMS regime on several grounds. For one, with the power to approve surveillance requests in the hands of only top-level officials, less attention will be dedicated to each individual surveillance request. Review of such requests will be inadequate because senior government officials will be inundated with interception requests that they have neither the time nor the manpower to evaluate.[61] Thus, the risk of erroneously authorizing surveillance requests is great. To make matters worse, the record of surveillance authorizations will be accessible only internally within the government. Where requests are improperly granted, the public has no way of knowing about them, let alone

---

it will be the same individuals issuing the orders in the first place. This is "[h]ardly a reassuring safeguard." *Id.*

56. *Kotoky*, *supra* note 7.

57. *Id*.

58. The new, streamlined CMS system was summarized by Maria Xynou at The Centre for Internet & Society as follows:

> Without any manual intervention from telecom service providers, the CMS will equip government agencies with Direct Electronic Provisioning, filters and alerts on the target numbers. . . . Essentially, the CMS will be converging all interception lines at one location and Indian law enforcement agencies will have access to them.

Maria Xynou, *India's 'Big Brother': The Central Monitoring System (CMS)*, THE CENTRE FOR INTERNET & SOCIETY (Apr. 8, 2013), http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system.

59. Arun, *supra* note 26, at 2.

60. Singh, *supra* note 4.

61. *Id.*

challenging them. The Indian government insists that an audit trail will exist; however, the officials reviewing it will be the same individuals issuing the orders in the first place.[62] Understandably, this is "[h]ardly a reassuring safeguard"[63] for Indian citizens.

IV. STIFLING SPEECH UNDER SECTION 66A

The threat CMS poses to privacy was even more worrying when considered in conjunction with the threat to free speech posed by IT Act Section 66A.[64] That section proscribed the sending of "offensive messages through communication service, etc."[65] Where the penetrating lens of CMS can be employed to see into citizens' private communications, Section 66A could be used to prosecute those communications with little to no legal restraint.[66]

Section 66A(a) made it an offense to send any information through a communication service that is "grossly offensive or has menacing character."[67] This section was problematic in that the term "grossly offensive" remained undefined and could thus provide no guidance to citizens as to its application.[68] Without notice of what constituted illegal conduct, compliance with Section 66A(a) became impossible. Furthermore, it remained unresolved whether the offensiveness of the communication should be adjudicated based on the person targeted by the communications, or by a "reasonable person," which is crucial to its interpretation.[69] The law was deemed "draconian" in that "the wording of the Section ma[de] it so vague as to be applicable to virtually anything

62. Nair, *supra* note 12.

63. *Id.*

64. Information Technology Act, § 66A.

65. *Id*.

66. Section 66A is "potentially applicable to anything said online," creating a danger "of it being used both selectively and indiscriminately against individuals, groups, rights activists, journalists, political dissenters et al." *Section 66A of the IT Act Violates the Constitution of India*, THE ECONOMIC TIMES (Dec. 7, 2012)), http://articles.economictimes.indiatimes.com/2012-12-07/news/35670648_1_section-66a-annoyance-or-inconvenience-reasonable-restrictions.

67. *Id*.

68. *See* Viswanathan, *supra* note 25. In striking down the law, the Indian Supreme Court declared that the definition of its offenses were "open-ended and undefined." Sriram, *supra* note 33.

69. Pranesh Prakash, *Breaking Down Section 66A of the IT Act*, CENTRE FOR INTERNET & SOCIETY (Nov. 25, 2012), http://cis-india.org/internet-governance/blog/breaking-down-section-66-a-of-the-it-act:

> [T]he term "grossly offensive" will have to be read in such a heightened manner as to not include merely causing offence. . . . Additionally, in order to ensure constitutionality, courts will have to ensure that "grossly offensive" does not simply end up meaning "offensive," and that the maximum punishment is not disproportionately high as it currently is.

anyone might find 'grossly' offensive or causing 'annoyance or inconvenience.'"[70] The section was described by lawyers as a "poor cut and paste job," which "fail[ed] to define a specific category (context) as defined in the laws from where it [] borrowed words."[71] The vagueness of Section 66A's language is comparable to that of the IT Rules, which

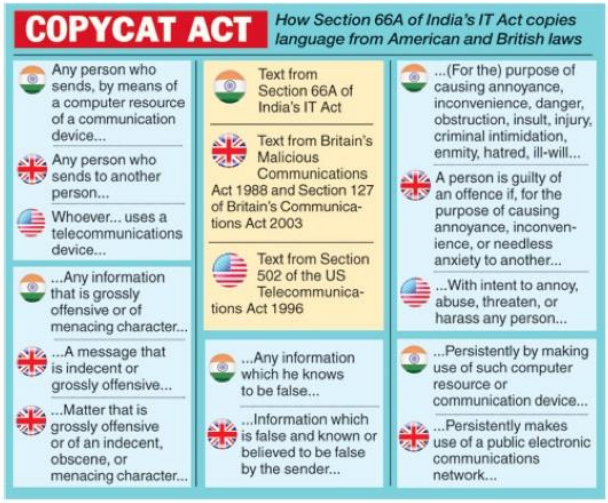
---

70. *Section 66A of IT Act Violates the Constitution of India*, THE ECONOMIC TIMES (Dec. 7, 2012), http://articles.economictimes.indiatimes.com/2012-12-07/news/35670648_1_section-66a-annoyance-or-inconvenience-reasonable-restrictions.

71. *See* G.S. Mudur, *66A "Cut and Paste Job,"* THE TELEGRAPH, (December 3, 2012), http://www.telegraphindia.com/1121203/jsp/frontpage/story_16268138.jsp. The Central Government defends Section 66A of the IT Act on grounds that it is derived from Section 127 of the U.K. Communications Act, which makes criminal the sending of "matter that is grossly offensive or of an indecent, obscene or menacing character." Communications Act of 2003 § 127. Importantly though, in Britain, unlike in India, the House of Lords has laid out a seminal test for "grossly offensive.". The test takes into account societal viewpoints and "all relevant circumstances." Director of Public Prosecutions v. Collins, [2006] UKHL 40 (U.K.), *available at* http://www.publications.parliament.uk/pa/ld200506/ldjudgmt/jd060719/collin-1.htm. The court observed, "[T]here can be no yardstick of gross offensiveness otherwise than by the application of reasonably enlightened, but not perfectionist, contemporary standards to the particular message sent in its particular context." *Id.* Critics of Section 66A urge that the provision should be "read down" in the same way in order to ensure that its application in India is kosher. Aparna Viswanathan urges:

> Instead of defending Section 66A on the grounds that it has been copied from U.K. legislation, the Union Government should take inspiration from the House of Lords' view about what is 'grossly offensive.' This is the standard that should be have been incorporated in the advisory issued by the Department of Electronics and IT.

Viswanathan, *supra* note 25. The language of 66A was also taken in part from Britain's Malicious Communications Act of 1988, intended to prevent the sending of malicious messages outside the scope of online communications, and the United States' Telecommunications Act of 1996. The following image provides a visual depiction of the legal language from which Section 66A was crafted:



Id.

prohibit the hosting of "objectionable," "hateful," "disparaging," and "defamatory" content[72] without defining those terms. The difference is that, unlike the IT Rules, which apply to ISPs, Section 66A applied directly to Indian citizens.[73] It could be used to target individuals for their speech rather than telecom corporations, which was a much greater threat to civil liberties.[74]

Section 66A(b) criminalized the sending through a computer resource or communication device (1) communication known to be false (2) for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will (3) communicated persistently.[75] The most obvious flaw in this provision resided in the second criteria, which acted as a catch-all for criminalizing all manner of communications.[76] The broad ambit of proscribed communication was of concern because it grouped together seemingly trivial communications causing "annoyance," "inconvenience," or "insult" with much more serious "injury," "danger," and "criminal intimidation."[77] The fact that results as trivial as "annoyance" or "inconvenience" were criminalized in the first place was troubling.[78]

The government used Section 66A to silence dissent on the Internet on numerous occasions. Individuals were arrested for their critical political

---

72. 2011 IT Rule 3(2).

73. The text of Section 66A provides that the law applies to "any person" who sends proscribed content. IT Act § 66A.

74. citation

75. Information Technology Act, *supra* note 20, at § 66A(b).

76. Pranesh Prakash, *Indian Surveillance Laws & Practices Far Worse than U.S.*, The Economic Times (June 13, 2013), http://articles.economictimes.indiatimes.com/2013-06-13/news/39952596_1_nsa-india-us-homeland-security-dialogue-national-security-letters.

77. For a more detailed argument regarding the unconstitutionally broad nature of $ 66A(b)(2), *see* Prakash, *supra* note 5. Prakash comments specifically that,

> That a lawmaker could feel that punishment for purposes this disparate belonged together in a single clause is quite astounding and without parallel (except in the rest of the IT Act). That's akin to having a single provision providing equal punishment for calling someone a moron ("insult") and threatening to kill someone ("criminal intimidation").

Id.

78. *Id.* Viswanathan's critique of Section 66A(b)(2) includes the following:

> Surely it cannot be a legitimate legislative objective to restrict freedom of speech in order to prevent annoyance or inconvenience? Can a democratic society criminalise the causing of annoyance, inconvenience, insult or ill will? Causing insult or ill will or enmity could be a criminal offence if it amounts to defamation. However, insulting someone or causing someone inconvenience *per se* cannot surely be a crime in itself either in the real or virtual world.

Viswanathan, *supra* note 25.

speech on social media,[79] and mobile phones and social media sites were shut down to prevent communal riots.[80] India's paternalistic approach to monitoring citizens' online activity was also apparent in the number of requests it submitted to Google for user data[81] and for removal of content.[82] An anonymous press release claimed, "We know the

---

79. Human Rights Watch provides a brief history of arrests made for political speech on social media sites:

> In April 2012, a university professor was arrested in West Bengal for circulating an email with pictures that poked fun at the state's chief minister. In September, police in Mumbai arrested a political cartoonist, Aseem Trivedi, for his work focusing on political corruption. In October, police in Ponducherry arrested a businessman for posting messages on Twitter questioning the wealth amassed by the son of the country's finance minister.
>
> In November, two girls were arrested in Maharashtra for a post on Facebook questioning the shutdown of their city following the death of a powerful political leader. Following the girls' arrest, the central government issued an advisory to all state governments requiring prior approval from senior police officers for all arrests under Section 66A. In May 2013, the Supreme Court directed all states to carry out the government's advisory, making it mandatory for police to seek clearance from high-ranking officials.

India: New Monitoring System Threatens Rights, *supra* note 13.

80. In 2012, the government asked social media sites, including Facebook and Google, to block links to "inflammatory content" following a riot in Mumbai that was incited by doctored images showing violence against Muslims and false reports of more violence to cause mass panic. *Working with government to remove inflammatory content: Google, Facebook*, INDIA TIMES (Aug. 21, 2012), http://timesofindia.indiatimes.com/india/Working-with-government-to-remove-inflammatory-content-Google-Facebook/articleshow/15589923.cms.

The Indian government claimed to have already blocked 250 websites with the controversial videos and images. Rama Lakshmi, *India blocks more than 250 Web sites for inciting hate, panic*, WASH. POST (Aug. 20, 2012), https://www.washingtonpost.com/world/india-blocks-more-than-250-web-sites-for-inciting-hate-panic/2012/08/20/aee0b846-eadf-11e1-866f-60a00f604425_story.html.

In addition, it sought to have 16 Twitter handles blocked, including "several that resemble the official account of the prime minister's office, including obvious parody accounts, as well as the handles of at least two journalists and right-wing opponents of the ruling Congress Party, such as Pravin Togadia of the far right Vishwa Hindu Parishad (VHP)." Talia Ralph & Jason Overdorf, *Is India's Government Becoming Big Brother?*, GLOBAL POST (May 9, 2013), http://www.globalpost.com/dispatch/news/regions/asia-pacific/india/120824/india-china-censorship-internet. Kanchan Gpupta, a right leaning journalist, commented:

> I don't think that the government has been particularly happy with the fact that somebody who [does not] endorse this government's policies, its performance, and the manner in which this government has carried out its constitutional responsibilities [has gained an internet following], and they were just looking for an opportunity to sort of try and shut my voice down.

Id.

81. "In 2012, India sent in 4,750 requests to Google Inc. for user data, the highest in the world after the United States." Kotoky, *supra* note 7. This number was up 52% from two years ago. Trivedi, *supra* note 5.

82. *See* Pranesh Prakash, *Invisible Censorship: How the Government Censors Without Being Seen*, THE CENTRE FOR INTERNET & SOCIETY (Dec. 14, 2011), http://cis-india.org/internet-governance/invisible-censorship.

> [O]ut of the 358 items requested to be removed from January 2011 to June 2011 from Google service by the Indian government (including state governments), only 8 were for hate speech

government today hates [the] public criticizing it," citing the recent arrests of people for tweeting or posting on Facebook as proof.[83] Additionally, reports have shown that one of India's clandestine organizations, National Technical Research Organizations ("NTRO") has exceeded its scope. The NTRO has tried to crack into the servers of Google and Skype and was recently accused of accessing government officials' emails without permission.[84]

India's Telecom Ministry attempted to curb criticism of Section 66A by issuing guidelines for its implementation. These required the approval of police officers ranked inspector general or higher in order to register complaints and require service providers to restrict content that is "grossly harmful," "disparaging," "harmful to minors in any way," or that "threatens the unity, integrity, defence, security, or sovereignty of India."[85] While many activists welcomed the new guidelines,[86] they were inconsequential absent amendment of the Act itself because they were non-binding.[87] If the Indian government were truly committed to reform, it would have amended the law before it was struck down.

Section 66A was a dangerous companion to CMS because it granted the government legal authority to prosecute those citizens that it snoops on with little to no restraint.[88] Not only can the central government see

---

and only 1 was for national security. Instead, 255 items (71 per cent of all requests) were asked to be removed for "government criticism."

Id.

83. *Everything You Need to Know About Indian Central Monitoring System (ICMS)*, Anon Insiders (May 5, 2013), https://anoninsiders.net/everything-you-need-to-know-about-icms-1956/.

84. 84. *See* Pranesh Prakash, *Indian Surveillance Laws & Practices Far Worse than U.S.*, THE ECONOMIC TIMES (June 13, 2013), http://articles.economictimes.indiatimes.com/2013-06-13/news/39952596_1_nsa-india-us-homeland-security-dialogue-national-security-letters, stating:

> Recent reports reveal India's secretive National Technical Research Organization--, created under an executive order and not accountable to Parliament--, often goes beyond its mandate and, in 2006-2007, tried to crack into Google and Skype servers, but failed. It succeeded in cracking Rediffmail and Sify servers, and more recently was accused by the Department of Electronics and IT in a report on unauthorized access to government officials' emails.

85. Advisory on Implementation of 66A of the Information Technology Act, 2000, DEPARTMENT OF ELECTRONICS AND INFORMATION TECHNOLOGY (Jan. 9, 2013).

86. Panesh Prakash, one of the most prominent critics of CMS and the IT Act, said "I think this is a great step forward. . . There is still a lot to be done, but for now I am content with the government's decision of wanting to monitor the situation on the ground." Preetika Rana & Margherita Stancati, *India Tightens Rules on Hate Speech Law*, WALL ST. J. (Nov. 29, 2012), http://blogs.wsj.com/indiarealtime/2012/11/29/india-tightens-rules-on-hate-speech-law/. The leader of the New Delhi-based Internet Democracy Project also welcomed the guidelines, but not without reservation. She claimed that she would press for changing the wording of the Act if the guidelines fail to make a significant impact. *Id.*

87. *Id.* ("'Without the law being amended these cosmetic changes are of no consequence,' argues Pavan Duggal, a Delhi-based lawyer and cybercrime expert.").

88. *See supra* note 39.

directly into the private communications of its citizens, it could use Section 66A to prosecute any communications that it does not approve of.[89] Section 66A is no longer in effect, but certain provisions of the Indian Penal Code still have the potential to curb free speech.[90] If past enforcement of Section 66A is any indication of the government's future practices, then lawful speech could easily be arbitrarily prosecuted moving forward using those penal code provisions.[91] Speech need not even be public now to prompt government prosecution. For example, the central government now has the capability to tease out a target individual's private email drafts; if it disapproves of the email content, it can pursue the individual for a communication that was never even sent.[92] Where Section 66A was once used to prosecute communications posted on social media, it can now be employed to reach the most private of exchanges.[93] Where the government once censored only public-facing or publicly accessible communications through ISPs using Section 69, it can now

89. Already, India has increasingly employed Strategic Lawsuits Against Public Participation, or "SLAPP suits," to chill contrary opinions of citizens. Ujwala Uppaluri, *On the Unfortunate Rise of the Indian SLAPP suit*, THE FREE SPEECH INITIATIVE (May 24, 2013), *available at* http://thefsiindia.wordpress.com/2013/05/24/on-the-unfortunate-rise-of-the-indian-slapp-suit/. Uppaluri describes SLAPP suits as having three primary features:

> *First*, there is always, and necessarily, a power imbalance between the parties in such cases: the plaintiff or complainant will always have greater and often disproportionately greater access to the resources necessary to enter and sustain a litigation, in addition to social, political or corporate power. . . .
>
> *Second*, there is always one object: to intimidate a target into silence or apology by way of legal action or the threat of it. . . .
>
> *Third*, SLAPP suits are always characterized by a flimsy, frivolous or even non-existent cause of action.

Id.

90. One advocate told the Economic Times, "[w]hile 66A was trying to cover defamation, it can still be done through civil law." *Legal experts have mixed responses over abolition of Section 66A*, THE ECONOMIC TIMES (Mar. 15, 2015), http://articles.economictimes.indiatimes.com/2015-03-25/news/60475374_1_section-66a-bengaluru-social-media. In particular, Sections 153 and 505 of the Indian Penal Code can still be used prosecute citizens for their online posts. *Section 66A quashed: Citizens can still be arrested for online posts*, THE TIMES OF INDIA (Mar. 25, 2015), http://timesofindia.indiatimes.com/india/Section-66A-quashed-Citizens-can-still-be-arrested-for-online-posts/articleshow/46683200.cms. Section 153 allows for prosecution of a person who makes a statement, either orally or in writing, that incites communal riots or provokes communal tension. *Id.* Violations are punishable by 6 months to one year in prison. *Id.* Section 505 proscribes the spreading of a rumor causing public disorder. *Id.* The penalty for Section 505 is up to three years of imprisonment. *Id.*

91. In fact, these Indian Penal Code provisions were invoked along with Section 66A in order to make arrests for offensive posts. *Id.*

92. This is a hypothetical I created to illustrate my point. But if you're looking for authority to support the government's ability to access private email drafts, then: *See supra* note 8 and accompanying text.

93. *See supra* Part I.

access even private speech.[94] As a result, a "chilling effect" on free speech will take hold in India under which citizens self-censor their private communications for fear of possible government reprisal.

V. THE "CHILLING EFFECT" IMPOSED BY CMS & SECTION 66A

"A chilling effect occurs where one is deterred from undertaking a certain action X as a result of some possible consequence Y."[95] The doctrine of the "chilling effect" is employed by jurisdictions having constitutional cultures of free speech and association,[96] and it applies to cases where "governmental laws and governmental (or private) activities are of a nature that—while not directly censoring free speech—nonetheless have the impact of *self-censorship*."[97] The classic example of the chilling effect can be observed in "excessively worded libel laws" like Section 66A of the IT Act. "[I]n order to keep on the right side of the law, citizens will end up refraining from engaging in completely legal and legitimate forms of speech."[98] Although CMS surveillance does not directly regulate or impede the freedom of expression or association, Section 66A was "a classic case of a law that would exercise a deeply chilling effect on free expression."[99]

Empirical evidence demonstrates that government surveillance programs like CMS and libel laws like Section 66A have a measurable chilling effect on the free expression of citizens.[100] Research on the

94. *Id.*

95. Monica Youn, *The Chilling Effect and the Problem of Private Action*, 66 VAND. L. REV. 1473, 1481 (2013).

96. The 'chilling effect' is used routinely in the United States, Canada, South Africa and the ECHR, to name just four jurisdictions. *The Chilling Effect in India*, INDIA CONSTITUTIONAL LAW AND PHILOSOPHY BLOG (Dec. 5, 2013, 5:57 PM), http://indconlawphil.wordpress.com/2013/12/05/the-chilling-effect-in-india/. Doctrinally, the chilling effect in the context of free speech has received very little recognition in India. It has been acknowledged in a few Delhi High Court cases and scattered observations have been made by the Madras and Karnataka High Courts; however, the phrase has most often arisen in other contexts such as rent control. *Id.* It is unclear why the doctrine has not taken root in India, because even India's southern neighbor Sri Lanka has acknowledged its significance. *Id*.

97. *Id.*

98. *Id.*

99. *Id.*

100. One survey showed that, post September 11, 2001, some Muslim Americans who believed they were being monitored by the U.S. government actually modified their Internet usage to avoid the government's intelligence programs (by either reducing or eliminating their Internet usage). Dawinder S. Sidhu, *The Chilling Effect of Government Surveillance Programs on the Use of Internet by Muslim Americans*, 7 U. MD. L. J. RACE RELIG. Gender & Class 375, 391–93 (2007). Another study demonstrated markedly less defamatory content in Australia—a democratic nation— compared with Malaysia and Singapore, where speech in news is constrained by the government, demonstrating the

psychological effects of widespread government surveillance has shown subjects to be "self-conscious and fearful," and such apprehension manifests in a culture of self-censorship.[101] In speaking on the psychological effects of surveillance, philosopher Sandro Gaycken posited that "[T]here are well-established psychological consequences to being watched. . . . People change, tailoring their behavior to fit what they believe the observer wants."[102]

The public continually witnessed the government's abuse of Section 66A to prosecute speech, and it may well see further abuses of the Indian Penal Code to the same end. As citizens learn that the government has real-time access to their phone calls, web browsing, and social media activity, intimidation will develop amongst the masses. Predictably, a culture of self-censorship will pervade. The public will become reluctant to disseminate ideas that may elicit disapproval from the central government, even if such ideas are legitimate, and even if those legitimate ideas are disseminated between private parties. This is because, under CMS, privacy in communications is a thing of the past. Citizens are exposed to the risk of being monitored each time they send an email, post content on social media, or make a phone call.[103] Such a risk may well outweigh the value of self-expression for many Indian citizens, who will cease to express their thoughts and opinions in order to avoid being targeted. In short, in the context of free speech and association, CMS will "stabilize[] totalitarianism, and destabilize[] democracy."[104]

VI. CMS WITHOUT PUBLIC REDRESS: BARRIERS TO PUBLIC OPPOSITION

CMS is threatening the vibrancy of free expression and eviscerating the right of privacy in India. Yet despite the magnitude of the rights at stake, much of the population in India lacks the ability to push back on the government by demanding transparency and accountability. Several forces

---

chilling effect of restrictions on free speech. Andrew T. Kenyon, *Investigating Chilling Effects: News Media and Public Speech in Malaysia, Singapore, and Australia*, 4 INTL. J. COMM., 440 (2010).

101. *See* Jillian C. York, *The Chilling Effects of Surveillance*, ALJAZEERA (June 25, 2013), http://www.aljazeera.com/indepth/opinion/2013/06/201362574347243214.html (observing the social toll of government surveillance in the Soviet Union or East Germany, referring to Marcus Jacob & Marcel Tyrell, *The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany* (July 26, 2010)).

102. John Boreland, *Maybe Surveillance is Bad, After All*, WIRED (Aug. 8, 2007), http://www.wired.com/threatlevel/2007/08/maybe-surveilla/ (discussing a pro-privacy speech given by Gaycken at an International Hacker Meeting). Gaycken further argued that the tendency of surveillance to create a "watched and a watching class" lends itself to totalitarianism. *Id.*

103. See Kotoky, *supra* note 7.

104. *Id.*

are at work in India that impede the conversation about CMS from getting started, and further barriers exist to prevent that conversation from gaining traction. Without a conversation, there cannot be collective action. Without collective action, a government will not be held accountable for its actions.

To begin with, the Indian public remains uninformed about CMS and its implications as the government's communication about the details of CMS has been extremely opaque. There is no public documentation explaining the "functions and technical architecture" of the program,[105] and public officials have refused to provide meaningful information about the program.[106] Government officials attempt to justify the secrecy of the program on grounds that public knowledge of CMS details would inhibit the effectiveness of the program's intelligence gathering.[107] Whatever the reason, Indian citizens cannot engage in meaningful conversation about a regime of which they are only vaguely aware. Until the government demonstrates more transparency, the Indian public is limited in its ability to advocate for enhanced privacy.[108]

Even those who know about CMS have virtually no rights to notice or due process in order to vindicate their privacy and free speech rights. Under the intermediary takedown system, the IT Rules do not require intermediaries to notify third parties whose expression is removed or

105. Acharya, *supra* note 25 (noting that the "lack of transparency is the single-largest obstacle to understanding the Central Government's motives in conceptualising and operationalizing the CMS"). The interception flow diagram of CMS remained under wraps as of this June. Singh, *supra* note 4.

106. Many public officials have chosen to remain anonymous when commenting about the reach of CMS and related privacy concerns. *See, e.g.*, Kotoky, *supra* note 7 (quoting a senior telecommunications ministry official who is directly involved in the program's set-up that "did not want to be identified because of the sensitivity of the subject.") Other officials have refused to comment at all. *Id.* ("A spokeswoman for the telecommunications ministry . . . did not respond to queries."). The Central Government attempted to show some accountability by enacting the National Cyber Security Policy ("NCSP") in July 2013; however, the NCSP is largely meaningless in that it does not even consider the effect that CMS will have on cybersecurity. *See* Acharya, *supra* note 14. In summarizing the problems with the NCSP, Acharya remarks,

> The NCSP's poor drafting, meaningless provisions, deficiency of analysis and lack of stated measures renders it hollow. Its notification into force adds little to the public or intellectual debate about cybersecurity and does nothing to further the trajectory of either national security or democratic freedoms in India.

Id. In a recent Google+ Hangout session, Milind Deora, India's Minister of State for IT, stated that "most people may not be aware of" CMS because it's "slightly technical." Trivedi, *supra* note 5. For video of the full Google+ Hangout, refer to http://www.youtube.com/watch?v=rwTsek5WUfE.

107. Kotoky, *supra* note 7.

108. Cynthia Wong, Internet researcher at Human Rights Watch, insisted that "[i]f India doesn't want to look like an authoritarian regime, it needs to be transparent about who will be authorized to collect data, what data will be collected, how it will be used, and how the right to privacy will be protected." *India: New Monitoring System Threatens Rights*, *supra* note 13.

blocked, nor do they require intermediaries to provide any explanation for declining or accepting takedown requests.[109] The situation can only worsen with the implementation of CMS, which completely removes intermediaries from the equation.[110] The government is not required to disclose any information about whom it is monitoring, so it will continue to deprive citizens of notice that their communications are being scrutinized.[111] Under CMS, the Indian public will remain in the dark about censorship activities and a buffer will no longer exist between the government and private communications. With no notice and even less procedural protection than before, citizens will find it nearly impossible to challenge the central government's invasive surveillance practices.

To make matters worse, the government has crippled organizations capable of educating Indian citizens about CMS and lobbying against it. The government recently clamped down on non-governmental agencies ("NGOs") receiving foreign funding,[112] posing a serious threat to the free speech and privacy movements in India.[113] Without funding from democratic nations that hold free expression in high regard, NGOs in India cannot operate to champion such democratic ideals on the ground. Without the support of these NGOs, Indian citizens lack a vehicle for advocacy. Most will either be unable or unwilling to speak out against CMS as individuals for fear of criminal prosecution.

In addition to regulatory barriers, several societal impediments in India obstruct public debate about CMS. For one, the lack of infrastructure and extreme poverty in India prevent millions from accessing digital forums

---

109. Dara, *supra* note 44 ("[T]he Rules are procedurally flawed as they ignore all elements of natural justice. . . . The Rules in their current form clearly tilt the takedown mechanism in favour of the complainant and adversely against the creator of expression.").

110. *See supra* note 43 and accompanying text.

111. *India: Big Brother up and running*, ENEMIES OF THE INTERNET, *available at* http://12mars.rsf.org/2014-en/2014/03/10/india-big-brother-up-and-running/.

112. *See* Rama Lakshmi, *Activists bristle as India cracks down on foreign funding of NGOs*, WASHINGTON POST (May 19, 2013), http://www.washingtonpost.com/world/asia_pacific/activists-bristle-as-india-cracks-down-on-foreign-funding-of-ngos/2013/05/19/a647ff80-bcaf-11e2-b537-ab47f0325f7c_story.html. The Indian government suspended the permission that Indian Social Action Forum (INSAF), a network of more than 700 NGOs across India receiving over 90% of its funding from foreign sources, had to receive foreign funds. "Anil Chaudhary, who heads an NGO that trains activists and is part of the INSAF network" stated, "The government's action is aimed at curbing our democratic right to dissent and disagree." *Id*. "The United States is the top donor nation to Indian NGOs . . . with Indian NGOs receiving funds from both the U.S. government and private U.S. institutions." *Id*. "In the year ending in March 2011 . . . about 22,000 NGOs received a total of more than $2 billion from abroad, of which $650 million came from the United States." *Id.*

113. NGOs as civil society groups "'are among the essential building blocks of any healthy democracy.'" *Id.* (quoting a United States State Department spokesman). By crippling them, the central government necessarily weakens democratic lobbying.

where public debate takes place. Only 12.6% of the Indian population has access to the Internet,[114] and only 3% of all households in India had a fixed Internet connection in 2012.[115] The extremely low level of Internet penetration can be explained in part by the following: lack of Internet infrastructure (i.e. few servers, low levels of PC ownership, lack of reliable electricity), extreme poverty in rural areas, and relatively high costs for broadband connections.[116] For most Indian citizens, Internet accessibility is only made available through cybercafés; however, the government imposed onerous regulations on cybercafés under the IT Rules[117] that stunt the growth of cybercafé facilities[118] and effectively restrict citizens' use of public Internet facilities.[119] Without access to the

---

114. Patry, *supra* note 40, at 17.

115. *Id.* "Only 2% of rural India has access to the web, according to the Internet and Mobile Association of India (IAMAI). That's a small percentage when you think that more than 70% of the population lives outside an urban conurbation." Rajini Vaidyanathan, *Is 2012 the Year for India's Internet?*, BBC NEWS (Jan. 3, 2012), http://www.bbc.co.uk/news/business-16354076.

116. CHANDRA GNANASAMNANDAM ET AL., ONLINE AND UPCOMING: THE INTERNET'S IMPACT ON INDIA, McKinsey & Company (Dec. 2012).

117. 2011 IT Rules. Privacy International has outlined the burdensome cybercafé regulations as follows:

> According to the new rules, cyber cafes are forbidden from allowing any user to use their computer resources "without the identity of the user being established." A user may establish his identify by producing any of seven different identity documents including driving license, passport etc. The cyber cafe is required to keep either a scanned copy or photocopy of the identity document produced and such a copy is to be retained for a period of one year. . . . The cyber cafe is required to maintain a detailed log of every user that includes the user's name, address, gender, contact number, type and detail of identification document, date, computer terminal identification, log-in time and log out time. For at least one year, the cyber cafe must also retain the complete history of websites accessed using computer resources at the cyber cafe and all logs of proxy server installed at cyber cafe. . . . The rules also stipulate the size of cubicles and their orientation.

India Country Report, PRIVACY INTERNATIONAL (Nov. 14, 2012), https://www.privacyinternational.org/reports/india-0.

118. *See* Nikhil Pawha, *Reasons for the Declining Growth of Cybercafes in India*, MEDIANAMA (July 17, 2008), http://www.medianama.com/2008/07/223-reasons-for-the-declining-growth-of-cyber cafes-in-india/ (discussing the various factors that impede the functioning of cybercafés, including numerous licensing requirements, "know your customer" norms, and police harassment, among others).

119. 'Cybercafé' has a very broad definition under the IT Act and means "any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public." IT Act 2011. This can include a wide range of venues beyond traditional cybercafés, including airports, hotels, etc. India Country Report, *supra* note 117. According to Melody Patry, the cybercafé rules are problematic for two primary reasons:

> Firstly, they limit the creation and sustainability of cybercafés by imposing draconian administrative requirements. For example, cybercafés must also have the capacity to retain user identity information and the log register in a secure manner for a minimum period of a year. Secondly, the rules directly limit citizens' access to cybercafés. Cybercafés cannot allow users to use computer resources without providing an established identity document, a barrier

Internet in the home or in public places, it is virtually impossible for Indian citizens to learn about, let alone participate in, the debate about free expression and the dangers of government surveillance. Even those with online access face communication barriers. "With over 30 major languages and 1500 dialects, India is a unique market."[120] Because there is no common language across India, it is difficult for Indian citizens to come together on free speech and privacy issues presented by CMS. Furthermore, most online content is English, which only 11% of the population can read.[121] The communication gaps created by language barriers will no doubt impede the free flow of ideas and opinions with regard to government surveillance.

An oppressive surveillance regime is taking hold in India, and yet its citizens have little to no power to fight it. The gravity of CMS's evils is compelling, but it is more worrying that citizens have almost no recourse, legally or otherwise. Without the means to unify and speak out against state monitoring, the world's largest democracy will devolve into the world's largest surveillance state.

VII. CONCLUSION

With the world's eye turned to government surveillance, there is no time like the present to confront the dangers of India's "Big Brother" CMS regime. The sheer magnitude of the threat to privacy and free expression in India is evident in the numbers. According to the Telecom Regulatory Authority of India, as of March 31, 2013 the number of telecom subscribers more than quadrupled from 2007, growing to 881.41 million total subscribers.[122] India is poised to see the world's largest incremental growth in Internet usage, from 330 to 370 million total users in 2015.[123]

---

for poorer people in rural communities who are disproportionately likely not to have the required identification.

Patry, *supra* note 40.

120. Shilpa Kannan, *Is Language the Key to Hooking India on the Web?*, BBC NEWS (July 8, 2012)), http://www.bbc.co.uk/news/business-18735792.

121. Patry, *supra* note 40.

122. Up from 205.87 total subscribers in 2007, this represents a compound annual growth rate of 43.93%. *Indian Telecom Sector Growth: An International Success Story*, PRESS INFORMATION BUREAU, GOVERNMENT OF INDIA MINISTRY OF COMMUNICATIONS & INFORMATION TECHNOLOGY (Dec. 23, 2011), http://pib.nic.in/newsite/erelease.aspx?relid=79183.

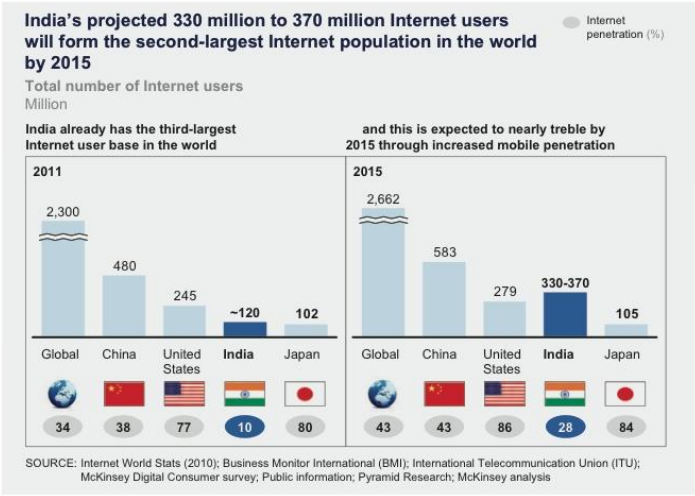
123. Gnanasamnandam et al., *supra* note 116. See chart below for graphical representation of India's projected growth in Internet users.

Even so, Internet penetration is quite low by global standards, as its 120 million users only account for 12.6% of the total Indian population.[124] It is shocking enough that this many telecommunications users are subject to government surveillance and censorship under CMS and the IT Act. But the number of *potential* users whose rights will be implicated by CMS is staggering. The telecommunications sector is flourishing in India like never before, and the central government is poised to seize it.

Where previously the government had to depend on ISPs to monitor and filter content, it can now tap directly into the private communications of its citizens. Its surveillance capabilities under CMS, combined with its prosecutorial power to regulate speech, previously under the ambiguous Section 66A and now under the Indian Penal Code, will create a chilling effect on free speech in India. The Indian people will no longer communicate freely for fear of arbitrary criminal prosecution, and a system of self-censorship will emerge. Governmental, infrastructural, and cultural barriers will likely impede public opposition to CMS, leaving Indian citizens largely without redress to vindicate their civil liberties. As such, reform of CMS and the IT Act depends in great part on the conversation outside of India. The Indian central government must be held accountable for its surveillance practices lest the democratic culture of free

---

Exhibit E1



expression be diminished. The fate of privacy and free expression in India lies with international activist organizations and other democratic nations who will demand accountability and transparency. Otherwise, the world's largest democracy could devolve into an Orwellian state.

Addison Litton[*]

---

* Executive Articles Editor, *Washington University Global Studies Law Review*; J.D. (2015), Washington University School of Law; B.S. in Business Administration (2012), University of South Carolina. Addison would like to express her gratitude to her classmates, family, and fellow Global Studies Law Review executive board members for making the notewriting process a formative one. Special thanks to Matthew K. Suess for his support and input at every stage of the process.