INDIA

	2012	2013
INTERNET FREEDOM STATUS	PARTLY FREE	PARTLY FREE
Obstacles to Access (0-25)	13	15
Limits on Content (0-35)	9	12
Violations of User Rights (0-40)	17	20
Total (0-100)	**39**	**47**

* 0=most free, 100=least free

POPULATION: 1.3 billion
INTERNET PENETRATION 2012: 13 percent
SOCIAL MEDIA/ICT APPS BLOCKED: Yes
POLITICAL/SOCIAL CONTENT BLOCKED: Yes
BLOGGERS/ICT USERS ARRESTED: Yes
PRESS FREEDOM 2013 STATUS: Partly Free

KEY DEVELOPMENTS: MAY 2012 – APRIL 2013

- Hundreds of blocks, supposedly targeting inflammatory content, affected a wide range of pages, including some in the public interest (see **VIOLATIONS OF USER RIGHTS**).
- At least eleven people were charged under Section 66 of the 2008 IT Act amendment for posts on social media (see **VIOLATIONS OF USER RIGHTS**).
- Cartoonist Aseem Trivedi was arrested for anti-corruption cartoons, initially on charge of sedition, which carries a life sentence (see **VIOLATIONS OF USER RIGHTS**).
- The Central Monitoring System, partly in place since April 2013, seeks to equip a range of agencies to monitor any electronic communication in real time, without informing the target or a judge (see **VIOLATIONS OF USER RIGHTS**).
- Online campaigning for women's rights in the wake of a brutal sexual assault promoted street protests and some legislative reforms (see **LIMITS ON CONTENT**).

INTRODUCTION

The internet has become a powerful tool for sharing information and articulating dissent in India, despite low overall penetration and power shortages limiting access for many. While still concentrated in urban areas, access is gradually spreading to rural India, providing a forum for voices not always represented in the traditional media.

There are no systematic restrictions on political content on the Indian web. Since the November 2008 terrorist attacks in Mumbai, however, a confusing and frequently contradictory series of legal amendments, rules, and guidelines have strengthened official powers to censor online content and monitor communications. A 2008 Information Technology Act amendment allowed officials to issue blocking orders to internet service providers (ISPs), outlining a procedure and protecting compliant companies from legal proceedings. But 2011 intermediary guidelines under the same Act introduced a different process, making companies liable to criminal penalties if they fail to delete or take down content which any individual flags as "offensive." Courts can also order blocks, and their efforts to contain copyright violations sometimes render entire platforms inaccessible. All told, hundreds of pages were reported blocked by multiple actors during the coverage period, most by the government grappling with religious unrest, though no formal count was made public. While some blocks targeted legitimate hate speech, the opaque process undermined public trust and left legitimate internet users, victims of "collateral blocking," without a means of appeal.

Twenty-five percent of India's internet users spent time on social media in 2012,[1] and this, too, is subject to unclear regulation under the amended IT Act's punitive Section 66. During the coverage period of this report, police arrested at least 11 people for social media posts—including tags, 'likes' and closed group comments—under the section's vague ban on annoying, offensive, or menacing messaging. Though most were swiftly bailed, the detentions—which often took place at night, involved defendants as young as 19, and in three cases in restive Jammu and Kashmir lasted 40 days—threatened the constitutionally-protected right to freedom of expression. Yet the IT Act's problematic provisions have yet to be reformed.

Security threats have also driven a frenzy of directives on surveillance in the past five years, including one ordering mobile providers to monitor all users' physical locations to within 50 meters, and others pushing international service providers that encrypt their users' communications to establish domestic servers that are subject to local law. In 2013, the government began transitioning to the secretive Central Monitoring System which will potentially empower a wide range of state agencies to access any electronic communication in India in real time, without service provider cooperation—though that cooperation is assured under license agreements. Surveillance requires no judicial oversight. While some of this activity might be justifiable, the lack of transparency surrounding the system, which was never reviewed by parliament, is concerning. The system's potential for abuse—already widely documented under the existing surveillance regime—is also disquieting, as is its inadequate legal framework. Outdated laws require case-by-case

[1] "25% Online Time Spent on Social Networks, 4 out of 5 Indians use Facebook," NDTV, August 20, 2012, http://bit.ly/PqAIGY.

clearance by high-level officials for wiretaps, for example, but are insufficient to regulate a system capable of mass location-based cellphone monitoring. Meanwhile, Indian citizens are surrendering more personal information—including biometric data, such as fingerprints—to electronic government databases than ever before. Yet no privacy law offers protection or redress if citizens' personal details or communications are improperly accessed. And while officials tout the centralized "electronic audit trail" the system creates each time it's used as a security feature, this data may itself be vulnerable to criminal infiltration.

As the country gears up for national elections in May 2014, these issues will become even more pressing. The main opposition Bharatiya Janata Party will take on the ruling Congress Party for control of the Lok Sabha, or lower house. The internet is already taking center stage, with both sides accusing the other of manipulating online discourse. There is no shortage of engaged civil actors countering the sometimes hostile online debate and advocating internet freedom. Whether the next government will be receptive remains to be seen.

OBSTACLES TO ACCESS

Internet usage in India continues to increase, with tens of millions of new users getting online each year. Internet penetration remains low by global standards, at 11 percent in December 2012, according to the Telecom Regulatory Authority of India (TRAI).[2] The International Telecommunications Union put penetration closer to 13 percent.[3] A pronounced urban-rural divide persists, and many people access the internet via cybercafes, as only 3 percent of households have an internet connection, according to recent census data.[4] A lack of local language content and applications also restricts penetration, though the situation is slowly improving.[5]

Overall mobile penetration was around 70 percent in 2012,[6] and mobile access is widespread, according to the Internet and Mobile Association of India, who reported in October 2012 that more than 90 percent of active urban internet users got online using a mobile device.[7] In January 2013, the government announced plans to allocate frequencies for a 4G network, which will further facilitate mobile web use.[8] Indians under 35 are 83 percent more likely to use mobile phones to go online at least once a week, compared to 55 percent of 50-64 year olds.[9]

[2] Telecom Regulatory Authority of India, "The Indian Telecom Services Performance Indicators April—June 2012," October 11, 2012, http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator%20Reports%20-%20Jun-12.pdf
[3] International Telecommunication Union, "Percentage of Individuals Using the Internet, 2000-2012," http://bit.ly/14IIykM.
[4] Hari Kumar, "In Indian Homes, Phones and Electricity on Rise but Sanitation and Internet Lagging," *India Ink*, *New York Times*, March 14, 2012, http://nyti.ms/1bhij8L.
[5] T. Ramachandran, "Soon, the Web Will Have .Bharat in Local Languages," *The Hindu,* March 8, 2013, http://bit.ly/VLN5St.
[6] Mobile penetration registered a slight decline from 72 percent in 2011, a reporting discrepancy due to large scale service disconnections in 2012. International Telecommunication Union, "Mobile-cellular telephone subscriptions, 2000-2012."
[7] IAMAI, "i-Cube IAMAI Urban Report 2012," September 27, 2012, available at Read Where, http://bit.ly/17cPPMC.
[8] "700MHz Spectrum Auction for 4G Services in 2014: Sibal" *Business Line, The Hindu,* January 21, 2013, http://bit.ly/V18xOC.
[9] "74% of the People with Mobile Phone Access Internet At Least Once a Week," *Moneycontrol,* November 26, 2012, http://bit.ly/1fyB2Sv.

Information and communication technologies (ICTs) have helped make education and other services more accessible and inclusive in India.[10] However, infrastructural limitations and cost restrict access, especially to broadband connections, which have overtaken dial-up as the primary access technology.[11] In particular, operators are reluctant to invest in their own tower networks, and rely instead on third-party services.[12] Cable-landing stations, where submarine cables meet the mainland, often impose hefty fees for allowing ISP traffic to pass in or out. There are 10 such stations, but the market is dominated by two players, Bharti Airtel and Tata Communications, which have a combined 93 percent market share.[13] ISPs also prefer to be physically close to international gateways, like the one in Mumbai, where the high cost of real estate drives up hosting prices.

Partly as a result of these challenges, the top 10 ISPs serve 95 percent of the total internet subscriber base. Few of the 104 service providers authorized to offer broadband have been able to penetrate the market given the strong position occupied by state-owned BSNL and MTNL.[14] Private companies have met with more success in the mobile phone service market. The top 10 providers are Bharti Airtel, BSNL, Vodafone Essar, Reliance Communications, Idea Cellular, Tata Communications, Tata Teleservices, Aircel, MTNL, and Tata Teleservices (Maharashtra) Limited (TTML).[15] Licenses are issued following a bidding process, but launching a mobile phone service business in practice requires considerable financial clout and access to important government officials. In a decision highlighting such tendencies and other corrupt practices in the telecommunications sector, the Supreme Court in February 2012 canceled 122 licenses for 2G mobile phone services. The licenses had been sold at artificially low prices in 2008 to a small number of favored firms.[16]

Broadband speeds remain slow in India. Testing by the technology firm Akamai in December 2012 indicated that the average connection speed in India was only 1 Mbps, an improvement from early 2012, but still slow by international standards.[17]

The government sought to address this through a National Telecom Policy unveiled in May 2012, focused on providing affordable and quality telecommunication services in rural and remote areas.[18] By promoting sustained adoption of technology, the policy seeks to overcome developmental challenges including access to education, health care and employment.

---

[10] Pallavi Priyadarshini , "A Quantum Leap with Virtual Classrooms," *New Indian Express*, April 22, 2013, http://bit.ly/XYKCpI.
[11] Rudradeep Biswas, "Fixed Services in India To Reach Rs 240 Billion in 2012, 2% Growth from 2011," *Telecom Talk,* July 23, 2012, http://telecomtalk.info/fixed-services-in-india-to-reach-billion-2012growth-from2011/97402/.
[12] "Need to Strengthen Telecom Infrastructure: Rakesh Mittal," *The Hindu,* December 6, 2012, http://bit.ly/XuJ1GB.
[13] Avinash Celestine, "Bandwidth Prices: Why We Pay More For Internet Services," *Economic Times,* March 31, 2013, http://articles.economictimes.indiatimes.com/2013-03-31/news/38163288_1_isps-doug-madory-providers/2.
[14] Telecom Regulatory Authority of India, *The Indian Telecom Services Performance Indicators: January–March 2010* (New Delhi: TRAI, July 2010), http://www.trai.gov.in/WriteReadData/trai/upload/Reports/51/finalperformanceindicatorReport9agust.pdf.
[15] "10 Top Telecom Service Providers in India," *Rediff*, August 9, 2010, http://bit.ly/1bhixwA.
[16] Vikas Bajaj, "Indian Court Cancels Contentious Wireless Licenses," *New York Times*, February 2, 2012, ttp://nyti.ms/19NBCn0.
[17] "India's Broadband Hits Speed Bump," *Business Line*, *The Hindu,* January 24, 2013, http://bit.ly/UZvRxS.
[18] Shalini Singh, "New Telecom Policy Seeks to Abolish Roaming Charges," *The Hindu,* May 31, 2013, http://bit.ly/16JHCvj.

While the cost of devices and data access is an obstacle to many in India, surveys indicate that lack of electricity, low digital literacy, and limited English are also major impediments. Inadequate power, in particular, is a key road block to internet adoption and usage.[19] India's average peak power shortage—the amount of electricity it failed to generate when consumption reached a maximum—was 9 percent between 2007 and 2012.[20]

Other government projects will benefit the ICT sector, such as the National Optical Fiber Network, an ambitious two-year proposal to bring broadband speeds of 100 Mbps to rural districts.[21] However, though pilot broadband networks are being developed in three states, the project is not on schedule for completion within the two years allotted, which concludes in November 2013.[22]

In addition to these nationwide challenges, select states battling insurgencies or other security threats are even more isolated. In the central states colloquially known as the red corridor—so-named for the simmering Maoist insurgency concentrated in remote, tribal areas—ICT investment is limited both by the conflict and the fact that other basic needs, such as drinking water and access to healthcare, are still unmet in many communities.

The national government can impose limits on ICT usage during times of unrest. In August 2012, officials limited SMS messages to five per user per day for fifteen days in an attempt to control religious tensions in the northeast.[23] State governments also occasionally respond to security challenges, interfering with connectivity by implementing shutdowns. In February 2013, the state of Jammu and Kashmir temporarily shut down mobile internet service when a prominent militant leader was executed.[24] Select village councils also occasionally banned women from using mobile phones on moral grounds. Though they affected a tiny fraction of the population, at least three such highly localized bans were imposed during the coverage period, one in July in Uttar Pradesh, one in August in Rajasthan that applied only to girls under the age of 18, and one in Bihar in December.[25]

The TRAI is the main telecommunications regulatory body, with authority over ISPs and mobile phone service providers. Established by parliament in 1997, it functions as an independent agency, offering public consultations and other participatory decision-making processes. The TRAI is generally perceived as fair. The Ministry of Communications and Information Technology and the Ministry of Home Affairs also exercise control over several aspects of internet regulation.

Cybercafes, initially straightforward to open and operate, are now regulated under 2008 amendments to the IT Act, which define them as any facility or business offering public internet

[19] "India still out of the Net", Debjani Ghosh, March 24, 2013. The Hindu Business Line , http://bit.ly/14hfEuu.
[20] "India suffered 9 pc peak power shortage during 2007-12: Economic Survey," February 27, 2013, http://bit.ly/13j9zh0.
[21] "Indian Government to Spend Rs 368 Billion on IT in 2013: Gartner," Channel World, February 5, 2013, http://bit.ly/1azx31S.
[22] "Bharat Broadband to Manage Optical Fibre Project" Thomas K Thomas, *The Hindu*, February 23, 2013, http://bit.ly/15kheug.
[23] Madeline Earp, "India's Clumsy Internet Crackdown," *CPJ Blog,* August 22, 2012, http://bit.ly/SofdHr.
[24] Committee to Protect Journalists, "Kashmir Restricts Cable TV, Internet Service," February 11, 2013, http://bit.ly/14T8agV.
[25] Lakshmi Sarah, "Women Banned from Using Mobile Phones in Indian Villages," *Global Voices,* December 8, 2012, http://globalvoicesonline.org/2012/12/08/women-banned-from-using-mobile-phones-in-indian-villages/.

access.[26] Obtaining a license can require approval from multiple agencies, though reporters in the city of Bangalore could not locate a single authority responsible for issuing it.[27] Some states levy license fees.[28] Regulations from 2011 oblige cybercafes to register, censor and monitor customers;[29] critics noted these requirements went beyond the IT Act provisions which prescribed them.[30] A March 2012 notice mandated each institution register for an official number,[31] a process distinct from licensing that overlaps with existing state or municipal laws,[32] but without specifying the timeframe, penalties for non-compliance or even the identity of the "registration agency" responsible. Some owners, already facing loss of revenue due to projected growth in personal connections, found the requirements burdensome.[33] Enforcement varied significantly around the country.[34]

LIMITS ON CONTENT

The government ordered ISPs to block hundreds of websites and URLs in an effort to contain religious unrest in 2012; whole platforms were affected in Jammu and Kashmir. Misguided court orders also resulted in content blocks—164 websites became inaccessible in just two days in February 2013. Corporate actors battling piracy caused ISPs to block entire video- and file-sharing sites. Intermediaries who fail to satisfy personal complainants offended by their content are liable to criminal and civil penalties under harsh guidelines that were subject to legal challenges during the coverage period. But despite civil society protests, reform has yet to materialize, while legal proceedings against several global internet companies are ongoing. Right-wing "Internet Hindus," that some say have political backing, had a negative impact on the online space in the past year, bombarding opponents with hostile comments. Women reported particularly aggressive electronic threats. Yet citizens also embraced digital tools to promote street protests after a brutal rape and murder in December 2012, prompting some legislative reforms.

Political censorship is by no means pervasive in India. It has increased, however, since a 2008 amendment to the IT Act granted the government power to block any content in the interests of defense, national security, sovereignty, friendly relations with foreign states, and public order.[35] The OpenNet Initiative reported no filtering of political and social content in India in 2007,[36] but

[26] Department of Electronics and Information Technology, "Information Technology Act," http://bit.ly/STh7NX.
[27] H.M. Chaithanya Swamy, "DNA special: Number of Licensed Cyber Cafes in City? Zero," *DNA India*, October 15, 2012, http://www.dnaindia.com/bangalore/1752626/report-dna-special-number-of-licensed-cyber-cafes-in-city-zero.
[28] "Cyber Cafes in Pune to Pay Licence Fees," *DNA India*, June 25, 2011, http://bit.ly/19dZZcD.
[29] Department of Information Technology, "Information Technology (Guidelines for Cyber Cafe) Rules, 2011," http://deity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.
[30] Bhairav Acharya, "Comments on the Information Technology (Guidelines for Cyber Cafe) Rules, 2011," Center for Information and Society, March 31, 2013, http://bit.ly/13KCBY5.
[31] Department of Information Technology, "Notification G.S.R. 153(E)," http://bit.ly/1dPHjoM.
[32] Bhairav Acharya, "Comments on the Information Technology (Guidelines for Cyber Cafe) Rules;" Debabrata Mohapatra, "Online Registration for Cyber Cafes, *Times of India,* May 8, 2013, http://bit.ly/1fyBDnk.
[33] Bhuvan Bagga, "Delhi Government to Watch Over Cyber Cafes," *India Today,* August 22, 2012, http://bit.ly/QopVsK.
[34] Sayantanee Choudhury, "Cybercafe Owners in Patna Violate Rules, *Times of India,* July 23, 2013, http://bit.ly/19K4QnT; "Police Vigilant Against Shoddy Cyber Cafes," *Times of India,* January 30, 2013, http://bit.ly/YnTOQp.
[35] Department of Electronics and Information Technology, "Information Technology Act."
[36] OpenNet Initiative, "India," 2007, https://opennet.net/sites/opennet.net/files/india.pdf.

selective blocking of both in 2012, while transparency surrounding the blocking process declined.[37] Religious and political extremist commentary was consistently targeted. Troublingly, "websites with information on human rights in India, internet tools such as proxies, and content related to free expression" were also selectively filtered. Blocks on pornography were fewer than those affecting other kinds of information.[38]

Though the 2008 amendment subjects the government's blocking authority to "procedure and safeguards," the 2009 rules which outlined these processes are inadequate, and not always followed in practice.[39] Service providers block websites at the behest of a committee of representatives from the ministries of law, justice, home affairs, information and broadcasting, and the cybercrime authority, the Indian Computer Emergency Response Team (CERT-In), which operates under the Department of Information Technology, often abbreviated as DIT. Citizens can't personally contact this group, but officials or police can submit vetted complaints on their behalf to the committee, who must give the person or intermediary who posted the contested information 48 hours to respond. Whether they do or not, the committee assesses the complaint, and sends those it considers legitimate to the IT department secretary for approval before directing service providers to implement blocks. The incumbent secretary is J. Satyanarayana.[40] In emergencies, he has the power to issue a temporary order directly if the committee subsequently reviews it within 48 hours. A review committee is expected to review all blocking decisions made under the law every other month.

Unfortunately, public misperceptions about this process undermine it in practice. Most news reports cite CERT-In as the authority behind website blocking, and the governmental department responsible as the Department of Telecom (DOT) based on earlier iterations of the act.[41] In fact, DOT has relinquished this authority to DIT, a subtle change barely clarified by the DIT's re-designation as the Department of Electronics and Information Technology (DEITY) in April 2012.[42] Meanwhile, CERT-In's power to authorize blocks passed to the committee outlined above. That body's name under rule 8(4) for section 69A of the 2008 act is "committee for examination of requests"—which can also be abbreviated as CER.[43] The imprecision surrounding these two entities is not just from the acronyms. Both CERT-In and CER are headed by the same person, Gulshan Rai.[44] The fact that he is empowered to sanction ISPs to block content is based on his role as the "designated officer" under the 2009 rules, rather than his position as director-general of the institution which manages cybercrime—though that institution, CERT-In, can issue requests to

[37] OpenNet Initiative, "India."
[38] OpenNet Initiative, "India."
[39] Department of Electronics and Information Technology, "Notification of Rules under Section 52, 54, 69, 69A, 69B," October 27, 2009, http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/Itrules301009.pdf.
[40] Department of Electronics and Information Technology, "People and Offices," http://deity.gov.in/content/people-and-offices.
[41] Department of Information Technology, "Ministerial Order on Blocking of Websites," July 7, 2003, *The Information Technology Act 2000,* (New Delhi: Universal Law Publishing, 2011) 156, http://bit.ly/1dPEKmD.
[42] "Department of Information Technology Renamed as Department of Electronics and IT," Press Trust of India via NDTV, April 18, 2012, http://bit.ly/HYXfoy.
[43] For the CER, see Pranesh Prakash, "DIT's Response to RTI on Website Blocking," Center for Information and Society, April 7, 2011, http://cis-india.org/internet-governance/blog/rti-response-dit-blocking. For pre-2008 rules, see;
[44] Sahil Makkar, "Gulshan Rai | We Believe in the Freedom of Speech and Expression," January 31, 2012, http://bit.ly/TtaW28. Rai was named India's first national cyber security coordinator in May 2013. It's not clear how this will affect his other roles. See, "Gulshan Rai to be first National Cyber Security Coordinator," *Indian Express,* May 10, 2013, http://bit.ly/148cJBC.

takedown or delete illegal content. This introduces further ambiguity, but regardless of how the authority is distributed between these groups, they all operate under the powerful Minister of Communications and Information Technology, Kapal Sibal, whose cabinet portfolio was extended in May 2013 to include the law ministry.[45] Popular criticism that content controls are too centralized may focus on the wrong institutions, but the underlying concern is often legitimate.

As in many democracies, the Indian judiciary is an independent arbiter of content disputes, and the government approves blocking orders submitted by the courts automatically. Regrettably, this gives local courts—who are often subject to social and political pressure, lack experience with internet issues, and can make rulings *ex parte,* meaning that they only hear one side of the case—considerable power to curb content. In some cases, service providers complied with blocking orders sent by lawyers informing them of a court decision, instead of an official notice, introducing additional scope for abuse.[46] In February 2013, Rai's committee instructed ISPs to block more than 70 URLs criticizing the Indian Institute of Planning and Management, a private business school, and its founder Arindam Chaudhuri, on the order of a district court in Madhya Pradesh, which was hearing a defamation suit filed by the institute.[47] One of the websites targeted belonged to the University Grants Commission,[48] which accredits higher educational institutions and refuses to recognize Chaudhuri's right to award degrees, a decision he characterized as defamatory.[49] Dozens of news articles reporting on the dispute, by *Outlook* magazine, the *Times of India,* the *Wall Street Journal* and the satirical website *fakingnews,* among others, were also blocked.[50] Since court orders are meant to be stayed by other courts, several news reports said the government would have to appeal against blocking that its own agencies had facilitated—one whose principle victim, the Commission, was a statutory body of the Indian government.[51]

Since 2011, a handful of higher courts have blocked content relating to copyright violations through particularly broad John Doe—or in India, Ashok Kumar—orders, which don't name a defendant.[52] These are not only pre-emptive—passed to prevent future violations of a movie that is not yet released—they are also misused by entertainment companies to make ISPs block entire platforms, whether or not they are hosting pirated material.[53] This was demonstrated in May 2012 when as many as 38 ISPs completely blocked a range of platforms, ranging from video site Vimeo to file-sharing websites; some reports said they were inaccessible for as long as a month.[54] The New Delhi-

[45] Anirudh Wadhwa, "A To-Do List for the New Law Minister," May 16, 2013, http://bit.ly/182ul3Y.
[46] Shalini Singh, "164 Items Blocked Online in Just 2 Days, Mostly on Court Orders," *The Hindu*, February 22, 2013, http://www.thehindu.com/news/national/164-items-blocked-online-in-just-2-days-mostly-on-court-orders/article4439917.ece.
[47] "Directed by Court, DoT Moves to Block 73 URLs Critical of IIPM," *Times of India,* February 15, 2013, http://bit.ly/XnqrPz.
[48] University Grants Commission, "Genesis," http://www.ugc.ac.in/page/Genesis.aspx.
[49] Urmi Goswami, "UGC Again Warns Students About IIPM," February 19, 2013, http://bit.ly/1hbu1CT.
[50] Danish Raza, "Glad Defamatory Links with Malicious Interests Removed: Arindam Chaudhuri," *Firstpost,* February 18, 2013, http://bit.ly/1bhiWiT.
[51] Shalini Singh, "164 Items Blocked Online in Just 2 Days;" "Govt Will Challenge Order to Block 78 Web Pages on IIPM," *Times of India,* February 20, 2013, http://bit.ly/ZvS63I.
[52] Kian Ganz, "[Update: Download Gangs of Wasseypur Order] Bombay HC Passes First Anti-piracy John Doe Order, as Law Firms Commoditise the New Vertical," *Legally India,* June 15, 2012, http://bit.ly/KIibkI.
[53] Apar Gupta, "Ashok Kumar is a Habitual Offender," *India Law and Technology Blog,* May 18, 2013, http://bit.ly/KsTdoC; Abhik Majumdar, "What's with this Kolaveri about John Doe Injunctions?" *Law and Other Things,* June 3, 2012, http://bit.ly/164cgUk.
[54] Anupam Saxena, "ISP Wise List Of Blocked Sites #IndiaBlocks," *Medianama,* May 17, 2012, http://bit.ly/JI5wlr; Software Freedom Law Center, "When Copyright Tramples on the Right to Freedom of Expression," July 2, 2012, http://bit.ly/19e0GCF.

based Software Freedom Law Center said Copyright Labs, an agency representing a movie production company, had interpreted an April court order from the Madras High Court in Chennai, state capital of Tamil Nadu, to allow absolute blocking, and that ISPs had complied; the court subsequently clarified that the order was only intended to affect specific URLs, not whole platforms.[55] Experts hope this clarification will encourage ISPs to contest widespread orders,[56] though some of the sites remained inaccessible even after the court's statement, and some news reports said more than 20 other John Doe orders issued by courts around the country are still open to wrongful implementation.[57]

These processes are not transparent for internet users, who are not informed of blocks until they encounter an error message—the 2008 IT amendment actually prohibits blocking complaints and decisions being made public. In some cases, error notifications cite a generic technical fault; in others, they add to confusion by citing an order from the DOT instead of DEITY. (Asked about one of these notifications, the DOT clarified that it was not responsible.[58]) In 2011, the Bangalore-based Center for Internet and Society obtained a list of 11 blocks via a freedom of information request, which it matched to 11 judicial orders.[59] Even then, there was no definitive way of confirming if the block came through via a court or DEITY—and consequently, no clear avenue for appeal. Results can even vary by ISP. Many rely on domain name system (DNS) tampering to stop users from visiting specific URLs or domains. In theory, this allows ISPs to interrupt the connection between an individual blog page and the person trying to retrieve it, and should not affect entire platforms. In practice, blocks are frequently overbroad, making it impossible to know which websites were targeted and which fell victim to collateral blocking.[60] In late 2012, the Toronto-based research group Citizen Lab reported three ISPs in India using PacketShaper technology, which allows more sophisticated blocking and throttling.[61] In April 2013, the *Economic Times,* citing minutes from a Home Ministry meeting, said the government planned to ask ISPs to segregate IP addresses by state to allow content blocking and monitoring on a regional basis.[62]

More nuanced filtering might seem like a welcome development in light of the court orders outlined above. In reality, it is cause for concern, given the disproportionate number of blocks ordered in the past year. In addition to the examples already considered, several hundred more pages were blocked based on communal or religious unrest. In August 2012, tensions between Muslims and non-Muslims in northeastern states including Assam, Karnataka, Tamil Nadu, and Maharashtra caused thousands to flee the region and sparked violence in cities around the country.

---

[55] Software Freedom Law Center, "When Copyright Tramples on the Right to Freedom of Expression."
[56] Nikhil Pahwa, "No More John Doe Orders? Indian ISPs Get Court Order For Specificity In URL Blocks," *Medianama*, June 20, 2012, http://www.medianama.com/2012/06/223-no-more-john-doe-orders-indian-isps-get-court-order-for-specificity-in-urls/.
[57] Prasad Krishna, "Reply to RTI Application on Blocking of Website and Rule 419A of Indian Telegraph Rules, 1951," Center for Information and Society, March 21, 2013, http://bit.ly/16JEbVd.
[58] Kul Bhushan, "Anonymous Takes Down IIPM Sites After DoT Blocks 'Defamatory URLs,'" *Think Digit,* February 18, 2013, http://www.thinkdigit.com/Internet/Anonymous-takes-down-IIPM-sites-after-DoT_13515.html.
[59] Pranesh Prakash, "DIT's Response to RTI on Website Blocking," Center for Internet and Society, April 7, 2011, http://cisindia.org/internet-governance/blog/rti-response-dit-blocking.
[60] OpenNet Initiative, "India," 2012.
[61] T. Ramachandran, "Indian ISPs Too Resorting to Censorship," *The Hindu,* February 9, 2013, http://bit.ly/1bhjlBC.
[62] Joji Thomas Philip, "Net Telephony Providers Will be Asked to Set Up Servers in India," *Economic Times,* May 20, 2013, http://bit.ly/15BHST3.

The government said that online hate speech, including falsified images of Muslims suffering violent attacks, was deliberately circulated to exacerbate the violence, and ordered blocks on at least 309 specific online items, a figure which was leaked to the press.[63] That number, which did not differentiate between blocks on entire platforms or individual URLs, was probably conservative, and the blocking was widely censured as indiscriminate.

Instead of combatting inflammatory content, the government's action disabled many objective sources of information, such as the Twitter handles of New Delhi-based journalists Shiv Aroor and Kanchan Gupta, who used their accounts to report on the unrest. News reports said that only a fifth of sites targeted mentioned the northeast, which undermined public trust in the action.[64] Officials accused Pakistani authorities of orchestrating online hate campaigns, adding a possible political motive for blocking. Other content, including a handful of political Twitter accounts such as @DrYumYumSingh, which spoofs Prime Minister Manmohan Singh, became inaccessible at the same time, although they were not on the leaked list, leading many to wonder if political critics were being singled out as well.[65] Other reports said Twitter had removed some accounts for violating user agreements.[66] In February 2013, the Press Trust of India said a "high-level government committee" had decreed that 306 blocks on Twitter accounts implemented during this period were lawful, while four were not. It's not clear which accounts were affected or whether this number related to the 309 items described above, most of which were not hosted by Twitter.[67]

Over 240 further URLs were reportedly blocked in November 2012 in relation to the anti-Islamic "Innocence of Muslims" video uploaded in the United States in September, which prompted protests by Muslim communities throughout Asia. Minister Sibal publicly announced the blocks, and said more were forthcoming.[68] Google separately reported having blocked access from India to several YouTube videos related to the "Innocence of Muslims" video, based on government request.[69]

Restrictions were more severe in the Muslim-majority state of Jammu and Kashmir, where militant groups seek political autonomy or union with Pakistan. After "Innocence of Muslims" caused mass protests in September 2012, residents of the state reported the blocking of several social networks, including Facebook and YouTube, as well as some disruption to e-mail, search engines, and Blackberry phone service; other mobile providers also blocked internet access altogether.[70] News reports said the state government ordered these shutdowns under Section 5(2) of the Indian Telegraph Act 1885, which shouldn't be possible, because it only pertains to the emergency

[63] Pranesh Prakash, "Analysing Latest List of Blocked Sites (Communalism & Rioting Edition)," Center for Internet and Society, August 22, 2012, http://cis-india.org/internet-governance/blog/analysing-blocked-sites-riots-communalism.
[64] Madeline Earp, "India's Clumsy Internet Crackdown."
[65] Pranesh Prakash, "Analysing Latest List of Blocked Sites."
[66] Kul Bhushan, "Facebook, Google to Help India Remove Hate Content; Twitter Blocks Fake Accounts," *Think Digit,* August 22, 2012, http://www.thinkdigit.com/Internet/Facebook-Google-to-help-India-remove-hate_10526.html.
[67] "Government Panel Okays Blocking of 306 Twitter Accounts," Press Trust of India, via *Times of India,* February 6, 2013, http://bit.ly/WSYZst.
[68] "Government Blocks 240 Weblinks Related to Provocative Film," Press Trust of India via NDTV, November 1, 2012, http://gadgets.ndtv.com/internet/news/government-blocks-240-weblinks-related-to-provocative-film-287053.
[69] Google, "India," July to December 2012, in *Transparency Report,* http://bit.ly/1biQu3o.
[70] "YouTube, Facebook Blocked on Mobile," *Greater Kashmir,* September 30 , 2012, http://bit.ly/QDF7Hq.

interception of electronic communications.[71] But while the state information and technology minister denied the order,[72] at least two service providers confirmed that there was a state-wide ban on Facebook and YouTube.[73] Service was subsequently restored. On February 14 and 15, however, DEITY ordered national blocks on more than 80 individual YouTube and Facebook pages after a Kashmiri sentenced to death for assisting with a Pakistani terrorist attack on India's parliament in 2001 was executed without warning or, critics said, due process.[74] *The Hindu* newspaper reported that the block was based on a court order procured by Jammu and Kashmir police.[75] Since these were implemented at the same time as the ones involving the business institute described above, Indian ISPs blocked 164 pages based on court orders in the space of two days, some due to a highly politicized conflict, others from private, commercial interests.

Administrative requests requiring service providers to take down content also spiked during these incidents. Facebook cooperated with the government during the northeastern unrest, though it was not clear how many pages were taken down as a result.[76] Twitter was asked to remove 20 accounts, but the extent of their cooperation was also unclear.[77] Google reported that removal requests from India in the second half of 2012 increased 90 percent compared to the first part of the year, notably from CERT-In during the northeastern riots, but the company did not comply with all.[78] While international companies often independently assess deletion requests to see if the flagged content violates local law or user guidelines before complying, domestic companies may be less discriminating. In March 2013, the Software Freedom Law Center said police ordered a web portal to delete an allegedly defamatory article under Section 91 of the penal code, which allows them to request information for the purposes of an ongoing investigation—even though the section does not provide for deletion of online content and is not applicable in defamation investigations. It was not an isolated incidence, the Center reported.[79]

Intermediaries are pressured into policing content by multiple actors. Both local and overseas companies are vulnerable to criminal prosecution if they fail to comply with complaints about content—not just from officials, but from anyone in India. The 2000 IT amendment made them liable for illegal content posted by third parties, though Section 79 of the 2008 amendment introduced some protections for companies and their customers.[80] In April 2011, however, Information Technology (Intermediaries Guidelines) Rules implementing the act undermined these protections—omitting, for example, any requirement to notify the person responsible for the censored material.[81] The guidelines, which cover internet and mobile service providers as well as

[71] Snehashish Ghosh, "Indian Telegraph Act, 1885," Center for Internet and Society, March 15, 2013, http://bit.ly/15Cdzq0.
[72] "Youtube and Facebook 'Blocked' in Kashmir," Al Jazeera, October 2, 2012, http://aje.me/PSPJjK.
[73] Kul Bhushan, "YouTube, Facebook Banned in Kashmir: Reports," *Think Digit,* October 1, 2012, http://bit.ly/W6Z4XA.
[74] Arundhati Roy, "Afzal Guru's Hanging Has Created a Dangerously Radioactive Political Fallout," *Guardian,* February 18, 2013, http://www.theguardian.com/commentisfree/2013/feb/18/afzal-guru-dangerous-political-fallout.
[75] Shalini Singh, "164 Items Blocked Online in Just 2 Days."
[76] "Working With Government to Remove Hateful Content: Facebook," Indo-Asian News Service via NDTV, August 21, 2012, http://www.ndtv.com/article/india/working-with-government-to-remove-hateful-content-facebook-257603.
[77] "India Faces Twitter Backlash over Internet Clampdown," Reuters, August 24, 2012, http://reut.rs/O8kGha.
[78] Google, "India."
[79] "S.91 of CrPC – the Omnipotent Provision?" Software Freedom Law Center, March 19, 2013, http://bit.ly/18zxqdo.
[80] Erica Newland, "Shielding the Messengers: Internet on Trial in India," Center for Democracy and Technology, March 20, 2012, https://www.cdt.org/blogs/erica-newland/2003shielding-messengers-internet-trial-india.
[81] Vikas Bajaj, "India Puts Tight Leash on Internet Free Speech," *New York Times*, April 27, 2011, http://nyti.ms/15BHZ0P.

web hosts, search engines and social networks, require them to disable access to offensive content within 36 hours of discovering it or receiving a complaint, either by blocking it or taking it down, or face prosecution leading to possible fines or jail terms.[82] A March 2013 clarification stated that acknowledging a complaint within 36 hours was sufficient if the content was disabled within a month.[83] This confused the process further, while doing nothing to address other glaring oversights.[84]

While the CER committee explicitly limited the power of private complainants, the Guidelines opened the floodgates. Any individual can complain to a service provider about content that they deem, for example, defamatory, disparaging, harmful, blasphemous, pornographic, promoting gambling or infringing proprietary rights.[85] None of these categories are defined. Experts say many violate the constitution by restricting legal speech—watching pornography, for example, is legal in India, and there are no limits on "disparaging,"[86]—a failing criticized by a parliamentary committee in March 2013.[87] Critics also objected to the 2011 rules telling cybercafes to stop users from accessing pornography on similar grounds; they were encouraged to install filtering software, although it's not clear how many complied.[88]

May 2012 amendments to the Copyright Act limited liability for intermediaries such as search engines that link to illegally-copied material, but mandated that they disable public access for 21 days within 36 hours of receiving written notice from the copyright holder, pending a court order to block or remove the link.[89] Rules clarifying the amendment in March 2013 appeared to give intermediaries power to assess the legitimacy of the notice from the copyright holder and refuse to comply, but critics said the language was too vague to restore the balance between the complainant and the intermediary.[90]

Civil society has been active in opposing the Intermediary Guidelines. In tests, the Center for Internet and Society demonstrated they could be used to render thousands of innocuous posts

[82] Ujwala Uppaluri, "Constitutional Analysis of the Information Technology (Intermediaries' Guidelines) Rules, 2011," Center for Internet and Society, July 16, 2012, http://bit.ly/1fRtyI2; Amol Sharma, "Is India Ignoring its own Internet Protections?" *Wall Street Journal,* January 16, 2012, http://on.wsj.com/xTjSiG.

[83] Department of Electronics and Information Technology, "Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011 under section 79 of the Information Technology Act, 2000," March 18, 2013, http://bit.ly/17cRimc.

[84] B. Singh, "Clarification On The Information Technology (Intermediary Guidelines) Rules, 2011 Under Section 79 Of The Information Technology Act, 2000," Center Of Excellence For Cyber Security Research And Development In India, April 4, 2013, http://perry4law.org/cecsrdi/?p=621.

[85] Ministry of Communications and Information Technology, "Information Technology Act, 2000," April 11, 2011, http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.

[86] Ujwala Uppaluri, "Constitutional Analysis."

[87] Ishan Srivastava, "Parliament Panel Blasts Govt Over Ambiguous Internet Laws," *Times of India,* March 28, 2013, http://articles.timesofindia.indiatimes.com/2013-03-28/internet/38098800_1_rules-self-regulation-pranesh-prakash.

[88] Javed Anwer, "No Access to Pornography in Cyber Cafes, Declare New Rules," *Times of India,* April 26, 2011, http://articles.timesofindia.indiatimes.com/2011-04-26/internet/29474462_1_cyber-cafe-cafe-owners-cubicles.

[89] Specifically, any providers offering "transient or incidental storage of a work or performance purely in the technical process of electronic transmission or communication to the public" through "links, access or integration." See, Pranesh Prakash, "Analysis of the Copyright (Amendment) Bill 2012," Center for Internet and Society, May 23, 2012, http://bit.ly/JSDMLg; Ministry of Law and Justice, "Copyright (Amendment) Act 2012," June 7, 2012, http://bit.ly/Kt1vlQ.

[90] Chaitanya Ramachandran, "Guest Post: A Look at the New Notice and Takedown Regime Under the Copyright Rules, 2013," *Spicy IP,* April 29, 2013, http://bit.ly/16zSzWf; Ministry of Human Resource Development, "Copyright Rules 2013," March 14, 2013, http://bit.ly/YrhCS5.

inaccessible.[91] Legal challenges are pending, including one submitted by a cyberlaw expert in Kerala in early 2012, who called them unconstitutional.[92] In April 2013, the Supreme Court agreed to reexamine them based on a petition by a consumer affairs website.[93] The site, MouthShut, which hosts user-generated reviews of products and services, said it had faced "hundreds of legal notices, cybercrime complaints and defamation cases" based on the rules, as well as calls from police officers to delete negative reviews.[94] The case is still pending.[95]

Other companies have been hit with criminal and civil charges even when there was no evidence that they were aware of the offending content, when they subsequently deleted it, or when they had no control over user-generated content hosted overseas by parent companies. Some of Google's mapping practices left the company's representatives liable for 3 years imprisonment, according to one expert.[96] In December 2011, journalist Vinay Rai filed a criminal complaint against 21 internet firms, including Facebook and Google, for hosting content he considered offensive, such as images depicting religious figures.[97] The charges invoked articles of the penal code that ban the sale of offensive material, including to minors, and punish criminal conspiracy.[98] Even under the broad auspices of the Intermediary Guidelines, the case had no foundation, because there was no evidence he had complained about the images. Some subsequently blocked the content, and others had charges dismissed on technical grounds,[99] but proceedings involving 11 companies were ongoing in May 2013.[100] Civil content complaints are also being heard by Indian courts, including one against several internet firms filed by Islamic scholar Aijaz Arshad Qasmi filed in December 2011.[101] Meanwhile, Facebook was subject to a police complaint in November 2012 for disabling an activist's account. The activist, based in Uttar Pradesh, said the closure was triggered by complaints from other internet users made in retaliation for his work.[102]

Individuals, as well as companies, are liable for third-party generated content. In 2009, the Supreme Court declined to quash a lawsuit against a student relating to third party comments in a group he created on Google's social network Orkut, rendering bloggers liable to civil or criminal

[91] Kirsty Hughes, "Internet Freedom in India—Open to Debate ," Index on Censorship, January 22, 2013, http://bit.ly/Xwxtxz.
[92] Prachi Shrivastava, "Read Parts of First Writ Challenging Censorious IT Act Intermediaries Rules in Kerala," *Legally India*, March 6, 2012, http://bit.ly/w4J7AN.
[93] Ashok Bindra, "Supreme Court of India to Examine the Validity of 2011 IT Rules Act," *TMC Net,* May 1, 2013, http://www.tmcnet.com/topics/articles/2013/05/01/336479-supreme-court-india-examine-validity-2011-it-rules.htm.
[94] Nikhil Pahwa, "MouthShut Challenges IT Rules In The Supreme Court Of India," *Medianama,* April 23, 2013, http://www.medianama.com/2013/04/223-mouthshut-it-rules-supreme-court-of-india/.
[95] "Stop Crying Wolf: Just Wait and Watch!" Software Freedom Law Center, August 23, 2013, http://bit.ly/12rUOqJ.
[96] S. Ronendra Singh, "Google Should Follow Indian Laws, say Rival Mapmakers," *The Hindu,* April 7, 2013, http://bit.ly/Y6hnQV.
[97] Amol Sharma, "Facebook, Google to Stand Trial in India," *Wall Street Journal*, March 13, 2012, http://on.wsj.com/x7z1ZT.
[98] Rishi Majumder, "The War on the Web is a War on Us," *Tehelka,* February 18, 2012, http://bit.ly/1bhno11.
[99] Pratap Patnaik and Bibhudatta Pradhan, "Indian Court Quashes Charges Against Microsoft on Content," Bloomberg, March 19, 2012, http://bloom.bg/x8qhvq; Kul Bhushan, "Web Censorship: Delhi Court Drops Google India, 7 Others From Lawsuit," April 13, 2012, http://www.thinkdigit.com/Internet/Web-censorship-Delhi-court-drops-Google-India_9279.html.
[100] "US Snubs India Over Case Against Google, Facebook," Press Trust of India via NDTV, May 3, 2013, http://bit.ly/104kAkV.
[101] Kul Bhushan, "Web Censorship Row: Delhi Court to Summon Facebook Via E-mail," *Think Digit,* April 20, 2013, http://www.thinkdigit.com/Internet/Web-censorship-row-Delhi-court-to-summon_9349.html.
[102] Prasant Naidu, Lucknow Lawyer Files FIR Against Facebook For Disabling His Account," *Lighthouse Insights,* November 20, 2012, http://lighthouseinsights.in/lucknow-lawyer-files-fir-against-facebook-for-disabling-his-account.html.

prosecution for comments posted by third parties.[103] No prosecutions have been reported since this ruling, but it may have encouraged self-censorship. Online journalists and bloggers approach certain topics with caution, including religion, communalism, the corporate-government nexus, links between government and organized crime, Kashmiri separatism, and hostile rhetoric from Pakistan.

The central authorities are not known to systematically employ progovernment commentators, but other factors exert a manipulative influence on digital discourse. Paid news, or "advertorials," are common in the traditional media in India, from unclear disclosure of paid endorsements to bribery and other kickbacks for coverage. In mid-2013, Indian digital media website *Medianama* reported this phenomenon had increased on digital platforms in the past three years.[104]

Of greater concern for political and social expression are the estimated 20,000 nationalistic "Internet Hindus" trolling websites to attack those who discuss sensitive topics online, some posting up to 300 comments a day.[105] While far from the only group with an agenda on the Indian web, they are "so numerous, so committed and can appear so organized" that they may have a disproportionate impact on legislators. Commentators note that official content regulation has occurred in step with the increase of aggressive, partisan debates being driven by national events like the 2008 terror attacks.[106] Some go further, tying the activity directly to the opposition Bharatiya Janata Party, who acknowledged operating 100 paid social media campaigners posting under multiple IDs in early 2013, but denied allegations that they "flood the internet with right-wing propaganda."[107] The ruling Congress party launched a rival online campaign in April but denied compensating participants. Internet users in India occasionally accuse individuals or media in Pakistan of manipulating discussions about the disputed Kashmir valley in domestic online forums, and some insurgent groups have also used digital tools to spread propaganda.[108] There is plenty of outspoken pushback against politicized trolling, but others may be deterred from expressing their views.

Many traditionally marginalized groups benefit from internet access to share information and connect with others, including Dalits, who are at the bottom of the Hindu caste system.[109] While rural and impoverished communities are underserved by internet access, mobile initiatives like CGNet encourage villagers to report news and information to the moderators of a central online

[103] Marshall Kirkpatrick, "Orkut User Loses in Indian Supreme Court," *ReadWrite,* February 24, 2009, http://readwrite.com/2009/02/24/orkut_user_loses_in_indian_sup#awesm=~ogYvZHQ5ELvHTf.
[104] Nikhil Pahwa, "Our Views On Paid News In Digital Media & Blogs In India," *Medianama,* June 21, 2013, http://bit.ly/17r8VRE.
[105] Jason Overdorf, "India: Meet the 'Internet Hindus,'" *Global Post,* June 18, 2012, http://bit.ly/Pac0bP.
[106] Ramachandra Guha, "Who Milks this Cow?" *Outlook,* November 19, 2012, http://bit.ly/Z25RV0.
[107] Kunal Pradhan, "Election #2014: As Cyber War Rooms Get Battle-Ready, BJP and Congress are Reaching Out to a New Constituency Spread Across Social Media," *India Today,* February 8, 2013, http://bit.ly/16DM9Rv.
[108] Rashmi Drolia, Chhattisgarh Cyber Police asks Facebook to Shut Down Maoist Page," *Times of India,* June 1, 2013, http://articles.timesofindia.indiatimes.com/2013-06-01/india/39673868_1_facebook-page-facebook-authorities-profile.
[109] Pramod K. Nayar, "The Digital Dalit: Subalternity And Cyberspace," *The Sri Lanka Journal of the Humanities 37* (1&2) 2011, available at Academia, http://www.academia.edu/1482588/THE_DIGITAL_DALIT_SUBALTERNITY_AND_CYBERSPACE.

forum via calls or SMS.[110] Begun in Chhattisgarh, the project has moved to nearby Madhya Pradesh and receives around 500 reports a day.[111]

Online activists are also vocal on internet freedom issues, such as the content regulation that followed the northeastern riots.[112] Charges against social network users under the IT Act's vague Section 66 also sparked strong public opposition, though these have yet to see effective results (see Violations of User Rights). Human rights issues spurred online actions during the coverage period, particularly in the aftermath of a shocking gang rape on December 16, 2012. Inspired by the success of a 2011 social media movement in support of anti-corruption campaigner Anna Hazare,[113] a number of social media campaigns became part of what some dubbed the *nirbhaya* ("fearless one") movement, helping propel women's rights onto the public agenda.[114] This helped drive public protests, which achieved some results when the government introduced two new pieces of legislation that parliament ratified in February and April, strengthening the legal penalties for sexual harassment.[115] However, others called for tighter regulation of online pornography as the driver behind the rise in sexual assaults against women.[116] The debate has yet to improve the online environment for women. Many say authorities are reluctant to recognize online threats and harassment as violations of the IT Act.[117] An all-female rock band in the Kashmir valley disbanded after online threats from radical religious groups.[118]

VIOLATIONS OF USER RIGHTS

Police around the country abused laws to threaten internet users during the coverage period. They were particularly active in Maharastra state, where blogger and cartoonist Aseem Trivedi was held for several days on sedition charges, and five people were detained for social media posts, sometimes in the middle of the night. At least eight more were charged for social media activity in other states under Section 66 of the IT Act, including three men in Jammu and Kashmir who were held for 40 days. Civil society opposition has yet to result in significant reform. Government surveillance, which requires no judicial oversight, is transitioning to a secretive, multi-million dollar Central Monitoring System, allowing officials to retrieve content and metadata from any electronic communication in India in real time, without the help of service providers. Much of the architecture of the system is already in place, and is scheduled to be fully operational by 2014,

[110] Preeti Mudliar, Jonathan Donner, and William Thies, "Emergent Practices Around CGNet Swara, A Voice Forum for Citizen Journalism in Rural India," Microsoft Research, March 2012, http://research.microsoft.com/apps/pubs/?id=156562.
[111] Elisa Tinsley, "In Rural India, a Hub for Tech, Mobile Innovation Gives Isolated People a Voice," International Journalists Network, September 5, 2013, http://ijnet.org/blog/rural-india-hub-tech-mobile-innovation-gives-isolated-people-voice.
[112] "Govt vs Twitter Provokes Angry Reactions, Hashtags like Emergency 2012," NDTV, August 23, 2012, http://bit.ly/OyHngx.
[113] Jaimon Joseph, "How Anna Hazare Became a Media Phenomenon," IBN Live, August 22, 2011, http://bit.ly/16JFofn.
[114] Shoma Chaudhary, "The Girl Who Fired an Outcry in India," *Daily Beast,* April 3, 2013, http://thebea.st/11V6lMR; Swasti Chatterjee, "8 Months After the Nirbhaya Case, Where Do We Stand?" *Times of India,* August 25, 2013, http://bit.ly/19NCqs5.
[115] Nagendra Sharma, "Two Bills, Two Punishments for Sexual Harassment," *Hindustan Times*, April 8, 2013, http://www.hindustantimes.com/India-news/NewDelhi/2-bills-2-punishments-for-sexual-harassment/Article1-1038995.aspx.
[116] Neha Thirani Bagri and Heather Timmons, "India Considers Banning Pornography as Reported Sexual Assault Rises," *New York Times,* April 22, 2013, http://nyti.ms/15CasOX.
[117] Divya Arya, "Why Are Indian Women Being Attacked on Social Media?" BBC, May 7, 2013, http://bbc.in/109OXot.
[118] "Kashmir Girls Pursue Career in Music Amid Fatwa," *Hindustan Times*, May 2, 2013, http://bit.ly/18eiNeJ.

despite never having been reviewed by parliament. Meanwhile, a privacy law proposed by experts in October 2012 has yet to be drafted.

Article 19 (1) of the Indian constitution protects freedom of speech and expression.[119] ICT usage is governed primarily by the Telegraph Act, the penal code, the code of criminal procedure, and the IT Act. Section 66 of the 2008 IT amendment punishes ill-defined "offensive," "menacing," or "false" electronic messages that cheat, deceive, mislead, or annoy, with jail terms of up to three years.[120] Experts say the Official Secrets Act has been used to limit expression in the past, and is not adequately balanced by the Right to Information Act.[121]

The Armed Forces Special Powers Act affects freedom of speech and expression in conflict zones, allowing security forces to bypass due process while shielding them from prosecution for human rights violations in non-military courts. Human rights groups and the international community have criticized the act, which is in effect in Jammu and Kashmir and several northeastern states, for compromising constitutional guarantees and protections.[122]

Criminal charges have been filed against cartoonists and journalists in relation to content published online. In September 2012, police in Maharastra arrested 25-year old cartoonist Aseem Trivedi, on charges of sedition—which carries a life sentence—as well as violating the Prevention of Insult to National Honor Act and the IT Act.[123] Trivedi was released on bail and the sedition charge was dropped after a public campaign, but the others remain pending.[124] Trivedi's anti-corruption cartoons first attracted official sanctions in December 2011 when his website *Cartoons against Corruption* was suspended by its hosting company based on a complaint to Mumbai police; Trivedi reposted the cartoons, which are widely available online.

While Trivedi's case was widely reported, local officials who abuse legal charges to suppress online reporting are less likely to be called to account. In May 2012, a district official in Jharkhand filed bribery charges against a video journalist who had submitted a right to information request about the use of public funds intended for job creation, apparently trumped up to pressure him to drop the investigation.[125]

Ordinary internet users in India also risk prosecution for online postings criticizing powerful figures. In April 2012, a professor at a university in West Bengal and several others were arrested for circulating a caricature via e-mail and Facebook that mocked a number of government officials,

[119] Government of India, "The Constitution of India," http://lawmin.nic.in/coi/coiason29july08.pdf.
[120] "Govt to Issue Fresh Guidelines to Prevent Misuse of Sec 66 (A)," Press Trust of India via *The Hindu,* November 29, 2012, http://bit.ly/19e28VH; Apurva Chaudhary, "Indian Govt Issues Guidelines To Prevent Misuse Of Sec 66A; PIL In Supreme Court," *Medianama,* November 29, 2012, http://bit.ly/SvBdiN.
[121] Iftikhar Gilani, "Government to review Official Secrets Act," *Tehelka,* October 15, 2011, http://bit.ly/1aztkkV.
[122] "Repeal AFSPA: UN Expert to India," Hueiyen News Service, May 2, 2013, http://e-pao.net/GP.asp?src=17..030513.may13
[123] Committee to Protect Journalists, "Indian Cartoonist Jailed for Images Criticizing Government," September 10, 2012, http://cpj.org/2012/09/indian-cartoonist-jailed-for-images-criticizing-go.php.
[124] Sumit Galhotra, "Sedition Dropped, but Indian Cartoonist Faces Other Charges," *CPJ Blog,* October 18, 2013, http://cpj.org/blog/2012/10/sedition-dropped-but-indian-cartoonist-faces-other.php.
[125] Committee to Protect Journalists, "Charges Against Indian Video Journalist Must be Dropped," May 25, 2012, http://cpj.org/2012/05/charges-against-indian-video-journalist-must-be-dr.php.

and charged under Section 66 of the IT Act as well as criminal defamation provisions of the penal code, before being released on bail.[126]

Abuse of Section 66 escalated during the coverage period, most notoriously in the western state of Maharashtra. On November 19, 2012, police in Palghar, a town in Thane district near the state capital Mumbai, detained two Facebook users for complaining that the funeral of Bal Thackeray, leader of the right wing Hindu party, Shiv Sena, was disrupting Mumbai services—an opinion shared by the Supreme Court, who ruled that bringing the city to a halt to observe the mourning was illegal.[127] Twenty-one year old Shaheen Dhadha posted the complaint and Renu Srinivasan 'liked' it, angering Shiv Sena supporters who gathered outside the police station and smashed a medical clinic belonging to Dhadha's uncle.[128] The detentions were widely criticized, both on social media and by public figures, and the women were released on bail within hours. Two policemen who ordered the arrest were suspended, the magistrate who granted them bail transferred, and the charges ultimately dropped, though Shiv Sena activists were still trying to challenge this decision in early 2013.[129] Yet the case had a disturbing coda. A Palghar branch of Shiv Sena launched a strike to protest the suspension of the two police officers, which was publicly criticized on Facebook under an account belonging to 19 year old Sunil Vishwakarma on November 28. Shiv Sena supporters delivered him to local police, who detained him for several hours, supposedly for his own protection. Vishwakarma denied authoring the comment, and police filed charges against an unknown individual for hacking his account.[130]

Journalists ferreting out other abuses of the act learned that Mumbai police had detained two Air India employees, Mayank Sharma and K.V. Jaganathrao, in May 2012 under Sections 66 and 67 on grounds that they made derogatory comments about politicians and insulted the national flag in a closed Facebook group.[131] The charges apparently stemmed from a personal spat with a colleague, Sagar Karnik.[132] The men said they were arrested in an overnight weekend raid and jailed for 12 days months after the complaint against them was filed.[133] Following media reports, police scrambled to rectify the situation by accepting a complaint from Jaganathrao about Karnick—also under Section 66 of the IT Act—for insulting his reputation on Facebook and Orkut.[134]

Other Section 66 charges were filed against social media users around the country during the coverage period. Many, like the Palghar girls, were young, like 22 year old Henna Bakshi and her friend, Kamalpreet Singh, charged by Chandigarh police in September 2012 for criticizing traffic

[126] Soudhriti Bhabani, "Professor Held for Uploading Caricature of Mamata on Social Site," *Daily Mail*, April 13, 2012, http://dailym.ai/19K2TYK.
[127] Julie Mccarthy, "Facebook Arrests Ignite Free-Speech Debate In India," NPR, November 28, 2012, http://n.pr/TuViZ3.
[128] Julie Mccarthy, "Facebook Arrests Ignite Free-Speech Debate;" "Two Girls Held for FB Post Questioning Bandh for Thackeray's Funeral," *Zeenews*, November 19, 2012, http://bit.ly/XsFr0A.
[129] "Palghar Court Closes Case Against Girls Arrested for Facebook Comments," Press Trust of India via NDTV, February 1, 2013, http://www.ndtv.com/article/india/palghar-court-closes-case-against-girls-arrested-for-facebook-comments-325157.
[130] "I Did Not Post on Raj Thackeray, FB Account was Hacked: Palghar Boy," *Firstpost,* November 29, 2012, http://bit.ly/18ej1CL.
[131] Jaganathrao was called K.V.J. Rao in some reports. Saurabh Gupta, "Arrested for Facebook Posts, They Spent 12 Days in Jail, Lost Their Air India Jobs," NDTV, November 25, 2013, http://bit.ly/1eQaRpk.
[132] "Cyber Police Station Files FIR Under 66A Against Sagar Karnik," *The Hindu,* December 3, 2012, http://bit.ly/15CaGFE.
[133] Meena Menon, "Jailed Air India Employees Demand Compensation," *The Hindu,* March 23, 2013, http://bit.ly/ZVPNDe.
[134] Saurabh Gupta, "Facebook Row: Mumbai Police Book Man Whose Complaint Led to Air India Employees' Arrests," NDTV, December 2, 2012, http://bit.ly/TCdOen.

officials.[135] Many were detained, usually briefly, and sometimes on grounds it would protect them, though this may well have amplified the impression that they were guilty of wrongdoing—especially when detentions occurred at night or bail was denied. Anti-corruption activist Ravi Srinivasan was arrested in his home in the union territory of Puducherry at 5am in October 2012 for offending a local politician on Twitter.[136] Orissa police arrested 20-year-old Pintu Sahu in December for posting an image of a Hindu deity sitting on a mosque on Facebook, representing a controversy between Mulsims and Hindus over a local shrine.[137] In February, police in Uttar Pradesh arrested Sanjay Chowdhary, a civil servant, for insulting a religious community and political leaders on Facebook, and denied at least one application for bail.[138] The most extreme case was in Jammu and Kashmir, where three men were arrested in October in connection with a video on Facebook, considered blasphemous, that spurred thousands of people to protest.[139] They were held for more than 40 days under the IT Act before being granted bail on December 12, although there was no evidence they had uploaded the video, which police said originated in Pakistan.[140]

The cases appeared to stall at the police level, without coming to trial. Yet legal arguments in bail hearings concentrated on proof—such as whether the police took screen shots of the offending posts—while the accused often blamed the content on hackers. This distracted from the fact that the charges themselves undermine constitutional free speech protections.

Section 66 faced numerous legal challenges in the past year. One petitioner told the Bombay High Court in 2013 that it should not apply to social media, which is mostly in the public domain, when the same content in print would not lead to prosecution.[141] Several members of parliament said they were working on amending it, though one motion to amend it was deferred pending a Supreme Court ruling.[142] The motion was revealing, however. In it, Member of Parliament P. Rajeev said that the 2008 IT amendment passed in the Lok Sabha in just seven minutes—along with six other bills—and went through the upper Rajya Sabha without discussion.[143] One inspiring challenge was filed with the Supreme Court in November 2012 by 21 year old student Shreya

[135] "Chandigarh Police Awaits Logs From Facebook in Abusive Remarks Case," *Indian Express,* September 20, 2012, http://m.indianexpress.com/news/chandigarh-police-awaits-logs-from-facebook-in-abusive-remarks-case/1005204/.
[136] Puducherry was formerly known as Pondicherry. Dhananjay Mahapatra, "Puducherry Justifies Arrest Under Section 66A of IT Act," *Times of India,* January 12, 2013, http://bit.ly/16zV4bY; Priscilla Jebaraj, "IAC Volunteer Tweets Himself into Trouble, Faces Three Years in Jail," *The Hindu,* November 1, 2012, http://bit.ly/16zV4bY.
[137] "Orissa: Youth Held for FB Photos of Hanuman on Mosque," *Outlook,* December 8, 2012, http://bit.ly/VEwiB3.
[138] "Man Held for Facebook Posts Denied Bail," Indo-Asian News Service via *Hindustan Times,* February 6, 2013, http://www.hindustantimes.com/India-news/UttarPradesh/Man-held-for-Facebook-posts-denied-bail/Article1-1007698.aspx.
[139] Arif Munshi, "Blasphemous Picture on Facebook Triggers Massive Protest," *Greater Kashmir,* October 29, 2013, http://www.greaterkashmir.com/news/2012/Oct/30/blasphemous-picture-on-facebook-triggers-massive-protest-27.asp.
[140] "Arrested For Video on Facebook, Three Men in Jammu and Kashmir Spend Over 40 days in Jail," NDTV, December 7 2012, http://bit.ly/SCmvH9; "India 2012 International Religious Freedom Report," in *International Religious Freedom Report for 2012,* Bureau of Democracy, Human Rights and Labor, United States Department of State, http://1.usa.gov/16zVajO.
[141] "Section 66A of IT Act Challenged as 'Unconstitutional', Court Seeks Center's Reply," Press Trust of India, February 28, 2013, http://bit.ly/WlM44R.
[142] Rajeev Chandrasekhar, "Don't Kill Freedom of Speech," *Times of India*, November 30, 2012, http://bit.ly/16zVf73; Apurva Chaudhary, "Indian Govt Issues Guidelines To Prevent Misuse Of Sec 66A; PIL In Supreme Court," *Medianama,* November 29, 2012, http://bit.ly/SvBdiN.
[143] P. Rajeeve, "Resolution Re. Need To Amend Section 66a Of Information Technology Act, 2000," December 14, 2012, available at Software Freedom Law Center, http://sflc.in/wp-content/uploads/2013/03/P.RajeeveResolution_RS.pdf.

Singhal.[144] Despite this activity, the sole, insufficient reform was a government advisory requiring senior police officers to approve arrests for social media postings, which the Supreme Court enforced in mid-2013, outside the coverage period of this report.[145]

State surveillance, like content control, is growing in scale and sophistication, and India's inadequate legislative framework provides almost no privacy protections. A 2007 Supreme Court ruling held that wiretapping would potentially violate constitutional protections under Article 19, the right to freedom of speech and expression and Article 21, the right to life and personal liberty, unless it was "permitted under the procedure established by law." The court ordered the creation of a government committee to review phone tap orders, which are governed by the Telegraph Act, but did not require judicial oversight.[146] A 2007 amendment was made to 419A Rules which govern the act, elaborating the procedure and limiting national and state home ministry officials of a certain rank to order phone taps.[147]

The amended 2008 IT Act also allowed both central and state officials to intercept, monitor or decrypt electronic communications or direct others to do so. Both this and the Telegraph Act stipulate surveillance should be done to protect defense, national security, sovereignty, friendly relations with foreign states, and public order, and that it should be subject to approval, limited to 60 days—fewer in emergencies—and renewable for a maximum of 180 days.[148] Yet the IT Act adds a clause allowing surveillance for "investigation of any offense;" moreover, while the procedure for high-level government authorization seems to involve a case-by-case assessment, systematic, mass surveillance is not prohibited.[149]

Additional requirements followed in 2011. The government authorized eight separate bodies to issue surveillance-related orders directly to service providers, from intelligence agencies to the tax bureau.[150] IT Act regulations required cybercafe owners to copy and retain customers' photo ID and browser history for a year.[151] Officials railed against international providers that prevent the government from tracking users by encrypting communications,[152] and required some, such as

---

[144] Bhadra Sinha, "SC Slams Facebook Arrests, Takes Up 66A," *Hindustan Times*, November 29, 2012, http://bit.ly/QOlCy2; Cordelia Jenkins, "Who is Shreya Singhal?" *Live Mint,* November 29, 2012, http://bit.ly/RkLiCm.

[145] J. Venkatesan, "No Blanket Ban on Arrests for Facebook Posts, says SC," *The Hindu,* May 16, 2013, http://bit.ly/1839Eou. "PUCL Leader Gets Bail in Facebook Post Case," *The Hindu,* May 14, 2013, http://bit.ly/129FnAB.

[146] Privacy International, "Chapter ii: Legal Framework," in *India,* November 14, 2012, http://bit.ly/17cVl1Q; Justice Ajit Prakash Shah, "Report of the Group of Experts on Privacy," October 16, 2012, http://bit.ly/VqzKtr.

[147] Jadine Lannon, "Rule 419A of the Indian Telegraph Rules, 1951," Center for Information and Society, June 20, 2013, http://cis-india.org/internet-governance/resources/rule-419-a-of-indian-telegraph-rules-1951.

[148] Jadine Lannon, "Indian Telegraph Act, 1885, 419A Rules and IT (Amendment) Act, 2008, 69 Rules," Center for Information and Society, April 28, 2013, http://bit.ly/14N1qCT.

[149] Pranesh Prakash, "How Surveillance Works in India," *New York Times,* July 10, 2013, http://nyti.ms/164b2sm.

[150] Research and Analysis Wing, the Intelligence Bureau, the Directorate of Revenue Intelligence, the Enforcement Directorate, the Narcotics Control Bureau, the Central Bureau of Investigation, the National Technical Research Organization and the state police. See, Privacy International, "Chapter iii: Privacy Issues," in *India Telecommunications Privacy Report,* October 22, 2012, https://www.privacyinternational.org/reports/india/iii-privacy-issues#footnoteref1_ni8ap74.

[151] "Information Technology Act, 2000," Ministry of Communications and Information Technology, April 11, 2011, http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.

[152] Joji Thomas Philip, "Can't Track Blackberry, Gmail: DoT," *Economic Times,* March 16, 2011, http://bit.ly/1bhkFo8; Joji Thomas Philip and Harsimran Julku, "E-services like Gmail, BlackBerry, Skype Can't be Banned for Lack of Scrutiny: Telecoms Security Panel," *Economic Times,* June 16, 2011, http://bit.ly/16TBotD.

Nokia and BlackBerry, to establish local servers subject to Indian law under threat of blocking their services.[153] (This effort was still ongoing in April 2013, when internal Home Ministry minutes suggested the government intends to require internet phone services like Skype to install local servers.[154]) Under a 2011 Equipment Security Agreement that did not appear on the DOT website,[155] telecom operators were told to develop the capacity to pinpoint any customer's physical location within 50 meters. "Customers specified by Security Agencies" were prioritized for location monitoring by June 2012, with "all customers, irrespective of whether they are the subject of legal intercept or not," by June 2014;[156] operators were in "various stages" of compliance by August 2012.[157] In October 2012, a government-appointed group described this framework as "an unclear regulatory regime that is inconsistent, nontransparent, prone to misuse, and that does not provide remedy or compensation to aggrieved individuals."[158]

Service providers are required by license agreements to cooperate with official requests for data.[159] Experts said that while non-compliance carries a possible seven year jail term, unlawful interception is punishable by just three years' imprisonment.[160]

Google and Facebook received more user data requests from India in 2012 than any other country except the U.S, but didn't always comply.[161] In January 2012, responding to a freedom of information request, the Home Ministry reported Indian officials issuing 7,500 to 9,000 phone interceptions per month.[162] During the coverage period, some news reports cited the "review committee" responsible for reviewing electronic interception orders every 90 days, established following the 2007 Supreme Court ruling and comprised of Cabinet Secretary Ajit Seth, Telecom Secretary R. Chandrasekhar and Legal Affairs Secretary B.A. Agrawal. In October 2012, *The Hindu,* citing this unnamed committee's "internal note," said interception involving 10,000 phones and 1,000 email IDs had been authorized by several agencies between June and August—some new, and some renewing existing orders.[163] In January 2013, the *Economic Times* said it had reviewed a

[153] In 2013, outside the coverage period of this report, BlackBerry confirmed their "lawful access capability" met "the standard required by the Government of India," though business customers would be unaffected. Anandita Singh Mankotia, "Government, BlackBerry Dispute Ends," *Times of India,* July 10, 2013, http://bit.ly/187FX9z. For Nokia, see Thomas K Thomas, "Despite India Server, IB Unable to Snoop into Nokia E-mail Service," *The Hindu,* July 14, 2011, http://bit.ly/1fRqjAt.
[154] Joji Thomas Philip, "Net Telephony Providers Will be Asked to Set Up Servers in India" *Economic Times,* May 20, 2013, http://bit.ly/15BHST3.
[155] Nikhil Pahwa, "New Telecom Equipment Policy Mandates Location Based Services Accuracy Of 50Mtrs: COAI," *Medianama,* June 17, 2011, http://bit.ly/keKNxY.
[156] Cellular Operators Association of India, "Additional Cost Implication for the Telecom Industry as Government Mandates Location Based Services to Meet its Security Requirements," press release, June 16, 2011, http://bit.ly/18zURS6.
[157] "Operators Implementing Location-based Services: Govt," Press Trust of India via NDTV, August 9, 2012, http://bit.ly/S4zNcT.
[158] Justice Ajit Prakash Shah, "Report of the Group of Experts on Privacy."
[159] Saikat Datta, "A Fox On A Fishing Expedition," *Outlook,* May 3, 2010, http://www.outlookindia.com/article.aspx?265192.
[160] Pranesh Prakash, "How Surveillance Works in India," *New York Times,* July 10, 2013, http://nyti.ms/164b2sm.
[161] "Indian Govt Snooped on 13 Users Per Day in 2012, says Google Report," Press Trust of India, March 11, 2013, http://bit.ly/Y5oepb; Facebook, "Global Government Requests Report," January—June 2013, http://on.fb.me/1dmxPnW. By contrast, India did not appear in the top five countries that made the most requests to Microsoft. See, Microsoft, "2012 Law Enforcement Requests Report," http://bit.ly/ZwBiGV.
[162] Shyamlal Yadav, "9,000 Orders for Phone Interception a Month: Govt," *Indian Express*, January 23, 2012, ttp://bit.ly/ylTTmN.
[163] Sandeep Joshi, "10,000 Phones, 1,000 E-mail IDs Under the Scanner," *The Hindu,* October 12, 2012, http://bit.ly/14T5EHr.

committee document covering October—December 2012, and involving surveillance orders for 10,000 phones and 1,300 emails.[164]

Abuse of surveillance has been widely reported, including monitoring of lawmakers, politicians, and journalists[165]—in one case, implemented by an ISP on the basis of an emailed government order that turned out to be fake.[166] In 2011, two senior Mumbai police officers were found to have sold phone records for money;[167] another in 2012 apparently requisitioned cell phone records "to keep an eye on his girlfriend."[168]

Much of this activity is driven by what *The Hindu* newspaper characterized as "massive purchases of communications intelligence equipment from secretive companies from India and abroad" by both state and other actors. Two suppliers are domestic: Clear Trail markets a "data traffic inspect engine" for mobile surveillance. Shoghi Communications supplies GSM monitoring and other equipment, but its only client is the government.[169] In 2010, *Outlook* magazine documented intelligence agencies operating dozens of cellphone monitoring devices that don't require the target's number—and therefore don't require cooperation from service providers. "We have deployed the system … in the hope that we might pick up critical conversations, but most of the time, we end up getting private calls," an unnamed intelligence official told *Outlook*.[170] Security agencies have even tried to limit the spread of these technologies. In 2011, the federal Intelligence Bureau was reported trying to shut down at least 33 passive interception units at internet hubs around the country. Many were being operated by state police with a tendency to misuse the equipment—or even mislay it.[171] On May 8, 2013, the Bureau issued a directive banning junior police officers from requesting mobile data records.[172] Yet the Bureau is itself a civilian organization without a statutory foundation or parliamentary oversight.[173]

Rather than correct this abuse, the government is transitioning to a nationwide surveillance project known as the Central Monitoring System (CMS), which allows government agents to bypass service providers in favor of interception equipment on intermediary premises allowing them to monitor electronic traffic on any platform or device directly, in real time.[174] Reports estimated the total cost was in the region of 8 billion rupees ($132 million).[175] Proponents said the system improved security by reducing the number of third parties involved in interceptions, and by documenting the

[164] Harsimran Julka and Joji Thomas Philip, "Home Ministry Ordered 10k Wire Taps in Last 90 Days, Orders Tapping of 1300 Email ids," *Economic Times,* January 3, 2013, http://bit.ly/XcPjaC.
[165] Saikat Datta, "We, the Eavesdropped," *Outlook*, May 3, 2010, http://www.outlookindia.com/article.aspx?265191; "800 New Radia Tapes," *Outlook*, December 10, 2010, http://www.outlookindia.com/article.aspx?268618; "Government Mulling Law to Regulate Phone Tapping," *DNA India*, December 16, 2010, http://bit.ly/eFX89N.
[166] Praveen Swami, "The Government's Listening To Us," *The Hindu*, December 1, 2011, http://bit.ly/rH8bO2.
[167] "Two Delhi Cops May Land in the Dock for Selling Cell Call Records," *Times of India*, March 11, 2012, http://bit.ly/1bhmHor.
[168] "Only Top Cops can Seek Call Records: State Intelligence Bureau," *Times of India,* May 17, 2013, http://bit.ly/1bhkSaX.
[169] Privacy International, "Chapter iii: Privacy Issues."
[170] Saikat Datta, "A Fox On A Fishing Expedition."
[171] Praveen Swami, "The Government's Listening To Us."
[172] "Only Top Cops Can Seek Call Records: State Intelligence Bureau," *Times of India,* May 17, 2013, http://bit.ly/1bhkSaX.
[173] A Subramani, Ex-officer questions Intelligence Bureau's legal status, *Times of India,* March 26, 2012, http://bit.ly/1aHbVKN.
[174] Anurag Kotoky, "India Sets Up Elaborate System;" Shalini Singh, "Govt. Violates Privacy Safeguards to Secretly Monitor Internet Traffic," *The Hindu,* September 9, 2013, http://bit.ly/1etaS0t.
[175] Pranesh Prakash, "How Surveillance Works in India."

nature and duration of requests in a streamlined "electronic audit trail."[176] But this may itself be vulnerable to cyberattacks.[177] It was never reviewed by parliament.

Some news reports said the eight agencies already empowered to conduct surveillance would be able to use it, with the addition of the National Investigation Agency, which was reported petitioning for inclusion in October 2012,[178] and possibly the Securities and Exchange Board of India.[179] Others said select military agencies would also be involved.[180] In April 2013, the Center for Information and Society submitted a freedom of information request to clarify the exact range of agencies authorized to conduct electronic surveillance, but had not received a response by the end of the coverage period.[181]

Operated by a little-known Department of Telecommunications unit, the Center for Development of Telematics,[182] it is not known how extensively the CMS has been implemented. One mid-2013 news report said it was active in New Delhi and neighboring Harayana state, with Kolkata, the capital of West Bengal, and the southwestern states of Kerala, Karnataka to follow.[183] Another said operation was yet to begin, pending technical certification of 21 regional monitoring centers.[184] But many internet and telecommunications firms already have monitoring capabilities installed, some of which are already controlled by the government, according to *The Hindu,* and the CMS will consolidate this equipment, too.[185] Since there is no legal requirement to notify the target of surveillance—even after the end of an investigation—its implementation may not be apparent, but several accounts said it would be fully operational by 2014.

Some of this activity, conducted to counter terrorism, is legitimate. But the surveillance architecture has been put in place without a privacy law, leaving individuals vulnerable, even as the kind of personal data they are surrendering to the government diversifies. Since 2010, millions of Indian citizens have been issued unique Aadhaar ID numbers as part of an anti-poverty initiative. Though not compulsory, officials say not possessing one could limit access to some government assistance. The authority that issues the numbers maintains a database of numbers tied to personal information including biometric data, such as fingerprints.[186] There is no law governing the authority—in fact, one was rejected by parliament in 2011.

---

[176] Bharti Jain, "Govt Tightens Control for Phone Tapping," *Times of India,* June 21, 2013, http://bit.ly/1bXQy3r.
[177] Anjani Trivedi, "In India, Prism-like Surveillance Slips Under the Radar," *Time,* June 30, 2013, http://ti.me/17cT6vA.
[178] Yatish Yadav, "NIA Seeks Central Monitoring System to Tap Phones," *Indian Express,* October 15, 2012, http://bit.ly/OAHjzx.
[179] "Govt to Install 'Fool-Proof' Phone Tapping Setup Soon," *Outlook,* June 17, 2013, http://bit.ly/1hbvWHu.
[180] Maria Xynou, "India´s 'Big Brother:' The Central Monitoring System (CMS)," Center for Internet and Society, April 8, 2013, http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system.
[181] Prasad Krishna, "RTI on Officials and Agencies Authorized to Intercept Telephone Messages in India," Center for Information and Society, July 15, 2013, http://bit.ly/1fRqJXu.
[182] "About C-DOT," http://www.cdot.co.in/rti/pdf/rti-2Inf-01a-AboutCDOT(E).pdf. News reports also said national Telecom Enforcement, Resource and Monitoring cells, also under the Department of Telecommunications, had a role in implementation. Department of Telecommunications, "TERM/Security," http://www.dot.gov.in/term/term-security.
[183] Shalini Singh, "India's surveillance project may be as lethal as PRISM," *The Hindu,* June 21, 2013, http://bit.ly/15EeV2o.
[184] Kalyan Parbat, "India's Surveillance System CMS to be Operational Soon," *Economic Times,* September 5, 2013, http://bit.ly/17QbPit.
[185] Shalini Singh, "Govt. Violates Privacy Safeguards."
[186] Nandan Nilekani, "The Science of Delivering Online IDs to a Billion People: The Aadhaar Experience," World Bank's Development Economics Lecture, April 24, 2013, http://bit.ly/15AS1O8.

In 2011, data protection rules improved privacy protections in commercial transactions but drew some criticism from the business community.[187] The EU does not consider India "data secure."[188] In October 2012, a group of experts issued a government-commissioned report providing a foundation for a future privacy bill, though the timeframe for drafting and implementing it isn't clear. Critically, this report clarified that exceptions to the right to privacy, such as national security and privacy investigations, be assessed according to values of proportionality, legality, and democratic rule.[189]

Violence targeting journalists, right to information activists and whistleblowers is common in India.[190] However, there were no significant accounts of physical assaults on bloggers or online activists during the coverage period. Some did face threats and pressure in retaliation for online activity. Many individuals facing charges under the IT Act, for example, were sought out by destructive mobs. Police and security agents were also accused of conducting violent raids while investigating alleged digital offenses, including some targeting cybercafe clients.[191]

Cyberattacks did not systematically target opposition groups or human rights activists during the coverage period. Loopholes in cyber security were exposed, however, when the international hacking group Anonymous targeted establishment sites, including that of the Supreme Court, in June 2012 to protest against decisions regarding file-sharing and copyright issues.[192]

[187] Outsourcing firms are exempt. Miriam H. Wugmeister and Cynthia J. Rich, "India's New Privacy Regulations," Morrison and Foerster Client Alert. May 4, 2011, http://bit.ly/lJSePF; John Ribeiro, "India Exempts Its Outsourcers from New Privacy Rules," *Network World*, November 2, 2011, http://bit.ly/16TCbuF.

[188] "India to EU: Declare us a Data Secure Country," Press Trust of India via *Times of India,* October 18, 2012, http://bit.ly/WCNAOh; Amiti Sen, "EU Not Ready to Give India 'Data Secure' Status," *The Hindu,* June 15, 2013, http://bit.ly/12wvF0g.

[189] Justice Ajit Prakash Shah, "Report of the Group of Experts on Privacy."

[190] Committee to Protect Journalists, "29 Journalists Killed in India Since 1992/Motive Confirmed," accessed August 2013, http://bit.ly/mnq7Mr; Prabhu Mallikarjunan, "Attacks on RTI Activists in India Raise Questions Over Safety Measures," *Indian Express,* January 17, 2013, http://newindianexpress.com/states/karnataka/article1423834.ece.

[191] Jaideep Mazumdar, "The Imphal Taliban," July 13, 2013, http://www.timescrest.com/opinion/the-imphal-taliban-10718.

[192] Rezwan, "India: Netizens Respond To Anonymous India's Protests," *Global Voices,* June 9, 2012, http://bit.ly/LbCEzI.