# INDIA

| | 2011 | 2012 |
|---|---|---|
| **INTERNET FREEDOM STATUS** | **Partly Free** | **Partly Free** |
| **Obstacles to Access (0-25)** | 12 | 13 |
| **Limits on Content (0-35)** | 8 | 9 |
| **Violations of User Rights (0-40)** | 16 | 17 |
| **Total (0-100)** | **36** | **39** |

* 0=most free, 100=least free

**POPULATION:** 1.3 billion
**INTERNET PENETRATION 2011**: 10 percent
**WEB 2.0 APPLICATIONS BLOCKED:** Yes
**NOTABLE POLITICAL CENSORSHIP:** No
**BLOGGERS/I USERS ARRESTED:** Yes
**PRESS FREEDOM STATUS**: Partly Free

## INTRODUCTION

Although India's internet penetration rate of less than 10 percent is low by global standards, the country is nonetheless home to over 100 million users, placing it third behind only China and the United States as of early 2012.[1] In the past, instances of the central government and state officials seeking to control communication technologies and censor undesirable content were relatively rare and sporadic. However, since the November 2008 terrorist attacks in Mumbai, which killed 171 people, the need, desire, and ability of the Indian government to monitor, censor, and control the communication sector have grown.[2] Given the range of security threats facing the country, many Indians feel that the government should be allowed to monitor personal communications such as telephone calls, email messages, and financial transactions.[3] It is in this context that Parliament passed amendments to the Information Technology Act (ITA) in 2008, expanding censorship and monitoring capabilities. This trend continued in 2011 with the adoption of regulations increasing surveillance in cybercafes. Meanwhile, the government and non-state actors have intensified pressure on intermediaries, including social media applications, to remove upon request a wide range of content vaguely defined as "offensive" and potentially pre-screen

[1] Eric Ernest, "India To Be World's Third Largest Internet Market," PC World, November 8, 2011, http://www.pcworld.in/news/india-be-worlds-third-largest-internet-market-57792011.
[2] Joshua Keating, "The List: Look Who's Censoring the Internet Now," Foreign Policy, March 24, 2009, http://www.foreignpolicy.com/articles/2009/03/23/the_list_look_whos_censoring_the_internet_now.
[3] "Security Forces, Media, 2 Pillars of Freedom: Poll," Times of India, August 15, 2010, http://timesofindia.indiatimes.com/home/sunday-toi/special-report/Security-forces-media-2-pillars-of-freedom-Poll/articleshow/6312697.cms.

user-generated content. Despite new comprehensive data protection regulations adopted in 2011, the legal framework and oversight surrounding surveillance and interception remains weak, and several instances of abuse have emerged in recent years.

The spread of information and communication technologies (ICTs) began accelerating in India with the liberalization of the telecommunications sector as part of the New Economic Policy in July 1991.[4] Throughout the early 1990s, various aspects of the telecommunications industry were opened to the private sector, including radio paging and mobile phones.[5] The government's New Telecom Policy of 1999 and New Internet Policy of 1998 have further spurred the growth of the ICT sector,[6] resulting in a large number of manufacturing units and internet service providers (ISP) setting up bases in the country.

## OBSTACLES TO ACCESS

Internet usage in India continues to increase, with tens of millions of new users getting online each year, though the penetration rate remains low by global standards. Infrastructural limitations and cost considerations restrict access to the internet, especially to high-speed broadband connections. According to the International Telecommunications Union (ITU), internet penetration was 10 percent—or about 120 million people—at the end of 2011.[7] Among internet users, 90 million were "active," accessing it at least once a month (70 million urban and 20 million rural).[8]

Many of India's users access the internet via cybercafes, as only 3 percent of households had an internet connection, according to recent census data.[9] The share of urbanite users with home connections has been constantly increasing and about 20 percent of urban households

[4] Invest India Telecom, "Indian Telecom Sector," Ministry of Communications and Information Technology–Department of Telecommunications, accessed January 3, 2011, http://www.dot.gov.in/osp/Brochure/Brochure.htm.
[5] Ibid.
[6] Telecom Regulatory Authority of India, "New Telecom Policy 1999," accessed January 3, 2011, http://www.trai.gov.in/TelecomPolicy_ntp99.asp; Peter Wolcott, "The Provision of Internet Services in India," in *Information Systems in Developing Countries: Theory and Practice*, ed. R. M. Davison and others (Hong Kong: University of Hong Kong Press, 2005), http://mosaic.unomaha.edu/India_2005.pdf.
[7] International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2011, accessed July 13, 2012, http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#.
[8] The Internet and Mobile Association of India (IAMAI) similarly reported that by September 2011 about 112 million Indians (9 percent of the population) had used the internet at least once in their lifetimes, and estimated this number would climb to 120 million by year's end. This was an increase from 77 million in 2010. See, IAMAI, "Report on Internet in India (I-Cube) 2011," 2011, http://www.iamai.in/Upload/Research/11720111091101/icube_3nov11_56.pdf.
[9] Hari Kumar, "In Indian Homes, Phones and Electricity on Rise but Sanitation and Internet Lagging," India Ink (blog), New York Times, March 14, 2012, http://india.blogs.nytimes.com/2012/03/14/in-indian-homes-phones-electricity-on-rise-but-sanitation-internet-lagging/.

possessed a computer in early 2012,[10] but there remains a pronounced urban-rural divide. Approximately 24 million rural residents used the internet in 2011, a rise from past years, but still only a tiny fraction of the total rural population of 800 million.[11] While cost is an obstacle, surveys indicate that lack of electricity, low computer literacy, and limited awareness of the internet are more significant.[12] Low literacy rates, particularly in English, are also a major impediment. The availability of internet content in India's eight most widely spoken languages is growing, but remains poor. After the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) approved the use of domain names in Hindi, Bengali, Punjabi, Urdu, Tamil, Telugu, and Gujarati,[13] the Indian government was preparing to roll out Hindi domain names in mid-2012, with other local language to follow.[14] U.S.-based software and internet giants Microsoft, Google, and Yahoo have launched initiatives to incorporate Indian languages into their programs and services.[15]

Broadband penetration is limited and slow. According to the Telecom Regulatory Authority of India (TRAI), as of December 2011 there were only 13.3 million broadband subscriptions in the country, most of them via ADSL rather than fiber-optic cable, contributing to lower speeds.[16] Testing by the technology firm Akamai in November 2011 indicated that the average connection speed in India was only 844 Kbps, an improvement from early 2011 but still low by international standards.[17]

The government and private companies are working to expand India's broadband infrastructure. According to a new telecom policy released in October 2011, the government plans to increase the number of broadband users to 175 million by 2017. One way they plan to achieve this is by pressuring cable television operators to shift from analog to digital services, so they can offer broadband internet via the same connections as cable TV

[10] Ibid.
[11] IAMAI, "Report on Internet in India (I-Cube) 2011."
[12] IAMAI, "84% of Rural India Not Aware of Internet," news release, September 13, 2010, http://www.iamai.in/PRelease_Detail.aspx?nid=2159&NMonth=9&NYear=2010.
[13] Surabhi Agarwal and Shauvik Ghosh, "Domain Names in Regional Languages Soon," Livemint.com, August 17, 2010, http://www.livemint.com/2010/08/17220818/Domain-names-in-regional-langu.html#.
[14] Surabhi Agarwal, "Hindi domain name to bridge digital divide," Livemint.com, November 4, 2011, http://www.livemint.com/2011/11/04005330/Hindi-domain-name-to-bridge-di.html.
[15] Ishani Duttagupta and Ravi Teja Sharma, "Google, Microsoft Focus on Regional Languages," Economic Times, August 2, 2010, http://economictimes.indiatimes.com/infotech/internet/Google-Microsoft-focus-on-regional-languages/articleshow/6242139.cms; Suw Charman-Anderson, "Yahoo India expands into five more Indian languages," Firstpost Technology, February 3, 2012, http://www.firstpost.com/tech/yahoo-india-expands-into-five-more-indian-languages-203034.html.
[16] Leslie D'Monte and Deepti Chaudhary, "Broadband user base still has a long way to go," Livemint.com, November 14, 2011, http://www.livemint.com/2011/11/14204650/Broadband-user-base-still-has.html?h=B; "Broadband Users at 13.3M; 3.4M Mobile Users Switch Cellular Operator in Dec," TechCircle.in, January 31, 2012, http://techcircle.vccircle.com/500/broadband-users-at-13-3m-3-4m-mobile-users-switch-cellular-operator-in-dec/.
[17] "Average connection speed in India stands at 844 kbps," Ciol.com, November 17, 2011, http://www.ciol.com/Technology/Networking/News-Reports/Average-connection-speed-in-India-stands-at-844-kbps/156663/0/.

subscriptions.[18] Plans to expand the country's international bandwidth may also yield increased speeds and lower prices.[19]

India's overall mobile phone penetration figures continue to grow at fast speeds, and an increasing number of Indians are also getting online via mobile devices. According to the TRAI and ITU, the total mobile phone subscriber base was 890 million by the end of 2011, including about 300 million in rural areas, an increase of 160 million subscribers compared to 2010.[20] Access to the internet through mobile phones has risen as well, apparently due to a series of inexpensive rate plans introduced in early 2010 and the long-awaited rollout of 3G services in early 2011 after years of bureaucratic delays.[21] According to the Internet and Mobile Association of India (IAMAI), of the 70 million active urban internet users, 26.3 million had access via their mobile devices in late 2011.[22] In March 2012, the government announced plans to allocate frequencies for a 4G network, which will further facilitate mobile web use.[23]

There were no reports of government-imposed internet connectivity disruptions in 2011 and 2012. However, in January 2012, mobile phone providers in Jammu and Kashmir shut off their services for one day as part of security precautions in place for Republic Day, reportedly due to fears that mobile phones could be used by terrorists to remotely detonate bombs.[24]

Three major operators sell international internet bandwidth at the wholesale level: Tata Group's VSNL, Bharti Airtel, and Reliance Globalcom. Since the deregulation of the telecommunications sector in the late 1990s, users in India have been able to choose among hundreds of different public and private service providers. BSNL and MTNL, both state owned, are the two largest ISPs, with a combined 70 percent of subscribers.[25] They retain a dominance established before the appearance of private competitors that each control under

[18] Bruce Einhorn, "India Seeks Access to the Broadband Highway," Bloomberg Businessweek, November 21, 2011, http://www.businessweek.com/magazine/india-seeks-access-to-the-broadband-highway-11172011.html.
[19] Rohin Dharmakumar, "The Long Arm of Broadband," Forbes India, February 5, 2010, http://business.in.com/article/breakpoint/the-long-arm-of-broadband/9592/1.
[20] "Broadband Users at 13.3M; 3.4M Mobile Users Switch Cellular Operator in Dec," TechCircle.in
[21] Bruce Einhorn, "After Years of Delays, India Finally Gets 3G," Bloomberg Businessweek, February 17, 2011, http://www.businessweek.com/magazine/content/11_09/b4217042858674.htm.
[22] IAMAI, "Report on Internet in India (I-Cube) 2011."
[23] "4G services: Govt to allocate airwaves in 700 MHz band," The Times of India, March 6, 2012, http://timesofindia.indiatimes.com/tech/news/telecom/4G-services-Govt-to-allocate-airwaves-in-700-MHz-band/articleshow/12159694.cms.
[24] "Republic Day: Mobile phone blackout in Kashmir," The Economic Times, January 26, 2012, http://economictimes.indiatimes.com/news/politics/nation/republic-day-mobile-phone-blackout-in-kashmir/articleshow/11637307.cms.
[25] TRAI, *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.

10 percent of the market.[26] Few of the 104 service providers authorized to offer broadband have been able to penetrate the market given the strong position occupied by BSNL and MTNL.[27] However, both companies have been forced to offer lower rates to stave off the private ISPs.

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).[28] 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.[29]

The TRAI is the main regulatory body for telecommunications matters, with authority over ISPs and mobile phone service providers. It functions as an independent agency, offering public consultations and other participatory decision-making processes. The TRAI is generally perceived as fair, though its reputation was tarnished by the above Supreme Court decision. The Ministry of Communications and Information Technology (MCIT) and the MHA also exercise control over several aspects of internet regulation, and interventions by the MHA in particular carry considerable weight. There have been no publicized disputes between the ministries and the TRAI to date.[30]

Although opening a cybercafe was relatively simple in the past, the authorities have complicated the process in recent years. Obtaining a license now requires approval from as many as six different agencies. New regulations passed in April 2011 require cybercafes to engage in more censorship, monitoring, and data storage (see details below), placing an additional burden on owners. These difficulties, combined with increases in home and mobile internet connections, have dimmed prospects for new entrants to the cybercafe market.

[26] Ibid.
[27] Nivedita Mookerji, "Stage Set for New Broadband Policy," Daily News & Analysis (DNA), June 11, 2010, http://www.dnaindia.com/money/report_stage-set-for-new-broadband-policy_1394639.
[28] "10 Top Telecom Service Providers in India," Rediff.com, August 9, 2010, http://business.rediff.com/slide-show/2010/aug/09/slide-show-1-10-top-telcos-in-india.htm#contentTop.
[29] Vikas Bajaj, "Indian Court Cancels Contentious Wireless Licenses," New York Times, February 2, 2012, http://www.nytimes.com/2012/02/03/business/global/india-supreme-court-cancels-2g-licenses.html?_r=1&ref=asia.
[30] B. Raman, "The Internal Security Czar," Outlook, December 24, 2009, http://www.outlookindia.com/article.aspx?263528.

## LIMITS ON CONTENT

As of early 2012, the Indian authorities blocked a small number of websites, including some with content in the public interest. More prevalent has been administrative censorship and requests for removal of content by both government and private actors. Such removals increased after passage of new regulations governing intermediary responsibilities in April 2011. Meanwhile, public debate intensified over the balance between free speech and protection of communities' religious sensibilities amidst a series of civil lawsuits—and at least one criminal case—against social media websites seeking to hold them responsible for content posted by users that some Indians found offensive.

Since 2003, the institutional structure of internet censorship and filtering has centered on the Indian Computer Emergency Response Team (CERT-IN), a body created in 2003 within the MCIT's Department of Information Technology (DIT). CERT-IN serves as a nodal agency for accepting and reviewing requests from a designated pool of government officials to block access to specific websites. When it decides to block a site, it directs the Department of Telecommunications—also part of the MCIT—to order all licensed Indian ISPs to comply with the decision.

In tests conducted in 2010 on four ISPs, the OpenNet Initiative (ONI) found selective, but consistent filtering of various extremist sites, as well as "websites with information on human rights in India, Internet tools such as proxies, and content related to free expression." The ISPs used DNS tampering[31] as their method of filtering, enabling targeted blocking of individual blogs, for instance, rather than an entire hosting service.[32] In April 2011, the Center for Internet and Society obtained a list of 11 banned websites from the DIT in response to a freedom of information request. All of the blocks were apparently implemented after a judicial order from a low-level court. For most of the websites, users encountered a technical error alert rather than a message explaining that inaccessibility was due to a court decision or government request.[33] Among the websites on the list were two related to the grassroots news organization Indymedia, a Facebook group called "I Hate Ambedkar" (a reference to B.R Ambedkar, one of the drafters of independent India's constitution), and Zone-H, an Italian security company serving as a repository for hacked

[31] According to ONI, "DNS tampering is the practice of preventing nameservers from returning the actual website requested by the user, and instead either showing an error page or explaining that it is blocked." See, Kendra Albert, "DNS Tampering and the ICANN gTLD Rules," OpenNet Initiative, June 23, 2011, http://opennet.net/blog/2011/06/dns-tampering-and-new-icann-gtld-rules.

[32] "India," OpenNet Initiative, December 2011, http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-india.pdf.

[33] Pranesh Prakash, "DIT's Response to RTI on Website Blocking," Center for Internet & Society, April 7, 2011, http://cis-india.org/internet-governance/blog/rti-response-dit-blocking.

websites.[34] Also blocked was an article on Bloggernews.net reporting about the Zone-H case.[35] Freedom House tests conducted in April 2012 indicated that the pages were still inaccessible from at least one major ISP. Regulations passed in April 2011 require cybercafes to equip computers with filtering software that blocks access to pornography or other "obscene information," though enforcement has reportedly been lax.[36]

Advanced web applications like the video-sharing site YouTube, the social-networking site Facebook, or the Twitter microblogging platform are freely available and becoming increasingly important in India. As of February 2012, Facebook was the third most popular site in the country, followed by YouTube at fourth, and Twitter at eleventh. In a dramatic drop, the social-networking site Orkut slipped from eighth to 37th.[37] With about 45 million Facebook users as of May 2012, India had the third largest subscriber base in the world, surpassed only by the United States and Brazil.[38]

In a bizarre incident in early 2011, some ISPs appeared to be blocking the websites of several smaller applications—including Typepad.com (a blog-publishing platform), Mobango.com (a mobile applications website), and ClickATell.com (a service for sending out bulk text-messages). Beginning on February 27, internet users reported being unable to access these websites, in some instances receiving a message stating, "This site has been blocked per request from the Department of Telecom."[39] Following a public outcry, Typepad was available again by the first week of March, though the other two sites remained inaccessible as of May 2012. The cause for the block remained unclear, as the Department of Telecom denied ordering it but did not provide any further explanation for the disruption.[40]

---

[34] The blocking of the latter emerged after a New Delhi court ordered CERT-IN to restrict access to Zone-H as part of a dispute with Indian security firm E2 Labs. Zone-H accused E2 Labs of inappropriately using its logo and E2 Labs responded by suing Zone-H for defamation. Zone-H claimed that it had not received sufficient notification to defend itself in court. See, Ketan Tanna, "Virtual Democracy?" Infochange Agenda, July 2011, http://infochangeindia.org/agenda/the-limits-of-freedom/virtual-democracy.html; Rahul Bhatia, "India Should Watch Its Internet Watchmen," Wall Street Journal, March 28, 2011, http://online.wsj.com/article/SB10001424052748704396904576226460167553174.html.

[35] Simon Barrett, "Blogger News Censored in India," Blogger News Network, July 12, 2012, http://www.bloggernews.net/124890; "Is E2 labs right in getting zone-h.org blocked?" Blogger News Network, March 12, 2012, http://www.bloggernews.net/124029.

[36] Aparna Viswanathan, "Big Brother is looking over your shoulders," The Hindu, October 13, 2011, http://www.thehindu.com/opinion/lead/article2532036.ece?homepage=true.

[37] "Top Sites in India," Alexa.com, accessed February 1, 2012, http://www.alexa.com/topsites/countries;0/IN.

[38] "India Facebook Statistics," Socialbakers.com, accessed May 1, 2012, http://www.socialbakers.com/facebook-statistics/india.

[39] Nikhill Pahwa, "Updatde: Indian Government Blocks Typepad, Mobango, Clickatell; Screenshots," Medianama.com, March 4, 2011, http://www.medianama.com/2011/03/223-indian-government-blocks-typepad-mobango-clickatell/.

[40] The claim was made in a response to a freedom of information request from civil society groups. Nikhill Pahwa, "#IndiaBlocks: India's IT Dept's Response To RTI Requests On Internet Blocking," Medianama.com, April 7, 2011, www.medianama.com/2011/04/223-indiablocks-indias-it-depts-response-to-our-rti-request-our-stand/; Pranesh Prakesh, "RTI Applications on Blocking of Websites," Center for Internet & Society, March 9, 2011, http://www.cis-india.org/internet-governance/blog/rtis-on-website-blocking; Priscilla Jebaraj, "Telecom Department orders ban on blog hosting site?" the Hindu, March 5, 2011, http://www.hindu.com/2011/03/05/stories/2011030564792200.htm; Rahul Bhatia, "India Should Watch Its Internet Watchmen."

More common than website blocking is the removal of content based on judicial orders, government directives, and citizen complaints. This phenomenon that has increased in recent years and in some cases, targeted content on political, social, and religious topics. Google's "Transparency Report" showed that the Indian authorities had submitted 68 removal requests covering 358 items between January and June 2011. According to Google, 255 items related to what it categorized as "Government Criticism," while 39 involved defamation and 8 pertained to hate speech. Google reportedly declined many of the requests, including one from "a local law enforcement agency to remove 236 communities and profiles from Orkut that were critical of a local politician," but in some cases it did restrict local access to "videos that appeared to violate local laws prohibiting speech that could incite enmity between communities."[41]

Bloggers are rarely forced by the government to take down their writings. However, in December 2011, the website "Cartoons against Corruption"[42] run by artist Asseem Trivedi was suspended by its hosting company after a lawyer filed a complaint to the Mumbai police that the site contained cartoons that "ridicule the Indian Parliament, the national emblem and the national flag."[43] Trivedi subsequently opened a blog on Google's Blogger platform where he reposted the cartoons.[44]

In April 2011, the government instituted Information Technology (Intermediary Guidelines) Rules, which require intermediaries—including search engines and social-networking sites—to remove content within 36 hours if an individual complains that it is offensive. The list of potentially offensive content is both wide-ranging and vague. It includes information that is "disparaging," "harmful," "blasphemous," "pornographic," "encourages gambling," "infringes proprietary rights," or "threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign states or public order."[45] Under the 2008 ITA, intermediaries in India are protected from prosecution for content posted by third parties, but according to the 2011 rules, they risk losing such immunity if they do not remove the offensive content within 36 hours of notification. Meanwhile, the rules do not provide an avenue for content producers to be informed of the removal or to contest the

[41] Google, "India," Google Transparency Report, accessed September 19, 2012, http://www.google.com/transparencyreport/governmentrequests/IN/.
[42] Original link: www.cartoonsagainstcorruption.com [site discontinued].
[43] Preetika Rana, "Cartoonist Faces Ban on Right to Poke Fun," India Real Time (blog), Wall Street Journal, January 4, 2012, http://blogs.wsj.com/indiarealtime/2012/01/04/cartoonist-faces-ban-on-right-to-poke-fun/?KEYWORDS=aseem+trivedi.
[44] "Ban on Website" [in Hindi], Cartoons Against Corruption (blog), accessed September 19, 2012, http://www.cartoonsagainstcorruption.blogspot.com/p/ban-on-website.html.
[45] "Information Technology Act, 2000," Ministry of Communications and Information Technology, April 11, 2011, p.12, http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf.

decision.[46] In March 2012, a cyberlaw expert in Kerala submitted a court petition challenging the constitutionality of the new regulations, specifically emphasizing the lack of transparency in the censorship process, even relative to more politically repressive countries like Saudi Arabia.[47]

In December 2011, Kapil Sibal, the Minister of Communications and Information Technology, introduced to the upper house of parliament controversial amendments to the Copyright Act, which critics complain would require internet companies to remove content flagged by other users as an infringement with little additional investigation.[48] The bill was pending at year's end and appeared unlikely to pass.

While most observers acknowledge that incendiary online content could pose a real risk of violence, particularly given India's history of periodic communal strife, press freedom and civil liberties advocates have raised concerns over the far-reaching scope of the ITA and the 2011 rules, their potential chilling effect, and the possibility that the authorities could abuse it to suppress political speech.[49] In December 2011, the Center for Internet and Society revealed the results of testing it conducted of intermediaries' responses to user requests to remove supposed "offensive" material.[50] The study found that rather than closely examining take down notice requests, intermediaries were erring on the side of caution and often over-complying.[51] This over-compliance was either due to their lacking the human resources to closely assess each complaint or fears of the legal and financial consequences of not removing remove material that might later be found to have been "offensive."

In late 2011, pressure was growing from some officials to take intermediary censorship to another level, such as requiring social networking sites to pre-screen user-generated content

[46] Vikas Bajaj, "India Puts Tight Leash on Internet Free Speech," New York Times, April 27, 2011, http://www.nytimes.com/2011/04/28/technology/28internet.html?_r=2&scp=1&sq=vikas%20bajaj%20Internet%20india&st=cse.

[47] Prachi Shrivastava, "Read parts of first writ challenging censorious IT Act Intermediaries Rules in Kerala," Legally India, March 6, 2012, http://www.legallyindia.com/201203062622/Bar-Bench-Litigation/read-first-writ-challenging-censorious-it-act-intermediaries-rules-in-kerala.

[48] "Kapil Sibal introduces Copyright Bill, Education Bills likely to suffer," The Economic Times, December 21, 2011, http://articles.economictimes.indiatimes.com/2011-12-21/news/30542786_1_education-bills-controversial-bills-copyright-bill; Pranesh Prakesh, "Invisible Censorship: How the Government Censors Without Being Seen," Center for Internet & Society, December 15, 2011, http://cis-india.org/internet-governance/invisible-censorship.

[49] Amol Sharma and Jessica E. Vascellaro, "Google and India Test the Limits of Liberty," Wall Street Journal, January 4, 2010, http://online.wsj.com/article/SB126239086161213013.html.

[50] For example, in six of the seven test cases, the intermediary removed the requested content and in several instances, more than what was asked for. See, Heather Timmons, "'Chilling' Impact of India's April Internet Rules," India Ink (blog), New York Times, http://india.blogs.nytimes.com/2011/12/07/chilling-impact-of-indias-april-internet-rules/; Pallavi Polanki, "How 'private-censorship' is making online content disappear, quietly," First Post India, December 15, 2011, http://www.firstpost.com/india/how-private-c ensorship-is-making-online-content-disappear-quietly-156545.html.

[51] Rishabh Dara, "Intermediary Liability in India: Chilling Effects on Free Expression on the Internet 2011," Center for Internet & Society, April 2012. http://cis-india.org/internet-governance/chilling-effects-on-free-expression-on-internet/intermediary-liability-in-india.pdf.

for potentially offensive information. Beginning in September 2011, Sibal, the Minister of Communications and Information Technology, held a series of meetings with leading internet companies, urging them to develop a voluntary code of conduct for removing content deemed offensive. Among the content of particular concern to the minister were reportedly webpages considered insulting to Prime Minister Monmohan Singh, ruling Congress party leader Sonia Gandhi, and religious leaders. The firms resisted, explaining that content which is legal and does not violate their policies will not be removed, even if it is considered controversial by some, and that a massive pre-screening process would be virtually impossible to implement. In December, Sibal suggested publicly that the government require internet companies to pre-screen and delete such content. The announcement sparked a flood of criticism from Indian media outlets, bloggers, internet experts, and civil society, many of whom questioned whether such a system would be constitutional.[52] In the face of the public outcry, no formal rules were introduced.

Nevertheless, the following month, the government sanctioned pursuit of a criminal case against 21 foreign internet firms including Facebook, Microsoft, Google, and Yahoo, accusing them of negligence for not removing offensive content. The case was initiated in December 2011 by a private citizen, journalist Vinay Rai, after he found content on their websites—including disrespectful images of the Prophet Mohammed or Hindu gods—and felt they offended Indians' religious sensibilities. If found liable, the defendants could face jail time or high fines. The government has drawn criticism for approving the prosecution although Rai had not first notified the companies, the process outlined under the 2008 ITA.[53] Google subsequently reported back to the court that it had removed the content in question from its search results, YouTube and Orkut social-networking site.[54] The case was still proceeding as of May 1, 2012.[55]

[52] John Ribeiro, "India May Overstep Its Own Laws in Demanding Content Filtering," PCWorld, December 5, 2011, http://www.pcworld.com/businesscenter/article/245548/india_may_overstep_its_own_laws_in_demanding_content_filtering.html.

[53] In January 2012, the internet firms lodged their own petition before the Delhi High Court asking it to quash the case. Meanwhile, the presiding judge told the companies to "develop a mechanism to check and remove offensive and objectionable material from their web pages," while warning that "Otherwise, like China, we may pass orders banning all such websites." In March 2012, the judge quashed the complaint against Yahoo and Microsoft, as they do not host user-generated content in the same manner. See, Amol Sharma, "Facebook, Google to Stand Trial in India," Wall Street Journal, March 13, 2012, http://online.wsj.com/article/SB10001424052702304537904577277263704300998.html; Andrew MacAskill and Pratap Patnaik, "Google, Facebook Seek Halt to Prosecution as India Objects to Some Content," Bloomberg, January 16, 2012, http://www.bloomberg.com/news/2012-01-16/google-facebook-seek-halt-to-case-as-india-objects-to-content.html; "Indian Court Threatens to Block Google and Facebook," Huffington Post, January 13, 2012, http://www.huffingtonpost.co.uk/2012/01/13/indian-court-threatens-to-block-google-and-facebook_n_1204005.html.

[54] Pratap Patnaik and Bibhudatta Pradhan, "Indian Court Quashes Charges Against Microsoft on Content," Bloomberg, March 19, 2012, http://www.bloomberg.com/news/2012-03-19/indian-court-quashes-charges-against-microsoft-in-content-case.html.

[55] Amol Sharma, "India Court Postpones Google, Facebook Censorship Hearing," Wall Street Journal, January 19, 2012, http://online.wsj.com/article/SB10001424052970204301404577170372338107512.html?mod=googlenews_wsj.

Internet companies have also faced several civil lawsuits over content deemed religiously offensive or defamatory. One high-profile case initiated by a Muslim cleric in December 2011 also targeted over 20 internet firms, including foreign social-networking sites.[56] Other cases lodged around the country focused on individual companies.[57] Taken together, the large number of suits, their continuation even after the offending content had been removed, and the apparent disregard for procedures outlined in the 2008 law have sent a chill through the IT sector. The cases have increased fears among IT firms large and small that they are vulnerable to frivolous legal action and could be held liable for not removing content posted by users even without receiving notification.[58]

Online discourse in India is vibrant, but online journalists and bloggers approach certain topics with caution. These include religion, communalism, the corporate-government nexus, links between government and organized crime, Kashmiri separatism, and hostile rhetoric from Pakistan. Such topics are addressed by online writers, but handled carefully to avoid inciting violence, particularly by non-state actors.

The Indian blogosphere is quite active and eloquent, complementing the rise in internet use by different interest groups and civil society actors, though the actual number of bloggers remains relatively small. A growing number of crowd-sourcing initiatives are being used to improve governance or counter societal harassment. Programs, often organized by non-governmental organizations, that enable reporting via text-message or online are tracking villagers' complaints, trash pick-up, bribery allegations, and incidents of sexual harassment.[59]

---

[56] Anuradha Shetty, "Google India, 7 others dropped from objectionable content lawsuit," Tech2, April 13, 2012, http://tech2.in.com/news/social-networking/google-india-7-others-dropped-from-objectionable-content-lawsuit/298102; "Court accepts Yahoo plea, fines complainant," Sify Finance, March 5, 2012, http://www.sify.com/finance/court-accepts-yahoo-plea-fines-complainant-news-national-mdfuEqaabbh.html?ref=false; "Google removes offensive content, Facebook says it doesn't control, operate servers," The Times of India, February 7, 2012, http://timesofindia.indiatimes.com/tech/news/internet/Google-removes-offensive-content-Facebook-says-it-doesnt-control-operate-servers/articleshow/11785178.cms; "Facebook India to court: Not responsible for user-generated content," The Times of India, February 29, 2012, http://timesofindia.indiatimes.com/tech/news/internet/Facebook-India-to-court-Not-responsible-for-user-generated-content/articleshow/12080208.cms.

[57] For example, in December 2011, an activist from Lucknow in Uttar Pradesh lodged a complaint against Facebook for posting comments that spread hatred against the sacred Hindu scripture Bhagavad Gita. Meanwhile, Google was facing a defamation case reportedly filed by an asbestos-manufacturing firm in Andhra Pradesh. See, "FIR against Facebook, user for anti-Gita comments," Daily Bhaskar, December 25, 2011, http://daily.bhaskar.com/article/UP-case-against-facebook-user-for-anti-gita-comments-2675251.html; Amol Sharma, "Google-Facebook Hearing Is Delayed in India," Wall Street Journal, May 3, 2012, http://online.wsj.com/article/SB10001424052702304743704577381790489739930.html. In January 2012, Facebook was forced to delete some allegedly defamatory content posted against Star News on a forum called "Fight against corruption in media."

[58] Amol Sharma, "Is India Ignoring its own Internet Protections?" India Real Time (blog) Wall Street Journal, January 16, 2012, http://blogs.wsj.com/indiarealtime/2012/01/16/is-india-ignoring-its-own-internet-protections/.

[59] Rama Lakshimi, "Indians use cellphones to plug holes in governance," Washington post, October 28, 2011, http://www.washingtonpost.com/world/asia-pacific/indians-use-cellphones-to-plug-holes-in-governance/2011/10/24/gIQAooAmOM_story.html.

The year 2011 also saw the emergence of a mass anti-corruption movement revolving around 76-year-old activist Anna Hazare, and propelled in large part by online media. As Hazare began a "fast to the death" in April 2011 to pressure the government to enact legislation that would create an effective, autonomous anti-corruption agency, news and support of his demands traveled quickly. Within days, his name became the most searched term on India's Google search engine, was trending on Twitter, and his Facebook page garnered 70,000 fans.[60] The movement grew to include dozens of protests and rallies across India. After ending his fast in August, Hazare turned to online media to directly communicate with his fans, launching a personal blog the following month with the help of aides, who say some posts have received over one million hits.[61] Although no new legislation had been passed as of May 2012, the government had promised to explore options.

## VIOLATIONS OF USER RIGHTS

The Indian constitution, particularly Article 19, protects freedom of speech and expression.[62] Along with the right to life and liberty under Article 21, Article 19(1) (a) has also been held to apply to the privacy of telephone conversations. Established guidelines regulate the ability of state officials to intercept communications,[63] but India lacks an appropriate legal framework and procedures to ensure proper oversight of intelligence agencies' growing surveillance and interception capabilities, opening the possibility of misuse and unconstitutional invasion of citizens' privacy.

ICT usage is governed primarily by the Telegraph Act, the penal code, the code of criminal procedure, and the ITA. The 2008 amendments to the ITA, which took effect in October 2009,[64] raised fears about an expansion of state surveillance capacity, including interception of email and mobile phone text messages. Several provisions of the revised law entail possible restrictions on users' rights, including classifying a broader scope of activities as criminal offenses.

Internet users in India have sporadically faced prosecution for online postings. In 2009, the Supreme Court ruled that both bloggers and moderators can face libel suits and even

[60] Samyuktha Krishnappa, "Social media support pours in for anti-corruption crusader Hazare in India," April 8, 2011, http://www.ibtimes.com/articles/132110/20110408/anna-hazare-fast-corruption-photos-video-social-media-internet-facebook-twitter-youtube.htm.
[61] Atikh Rashid, "Anna is new kid on the blog, and he is loving it," Express India, October 24, 2011, http://www.expressindia.com/story_print.php?storyId=864395.
[62] Government of India, "The Constitution of India," As modified up to the 1st December, 2007, http://lawmin.nic.in/coi/coiason29july08.pdf.
[63] *PUCL v. Union of India* (1997) 1 SCC 301. See also Vikram Raghavan, *Communications Law in India* (London: LexisNexis Butterworths, 2007), 760–761.
[64] The amended act is available at http://www.naavi.org/ita_2008/ch1_2008.htm, accessed September 19, 2012.

criminal prosecution for comments posted by other users on their websites. In April 2012, a professor at a university in West Bengal and several others were arrested for circulating a caricature via email and Facebook that mocked a number of government officials, including the railway minister.[65] They were charged under the ITA and criminal defamation provisions of the penal code, but released on bail.[66] In a troubling sign, at least two other ministers told media they supported the police action. No other high-profile arrests for online offenses were reported in 2011 or early 2012.

The overall level of ICT surveillance in India remains unclear, though it is believed to have grown in scale and sophistication since the Mumbai terrorist attacks in 2008. A series of scandals and new measures in recent years have exacerbated concerns over the lack of a legal framework or parliamentary oversight to regulate such activities. Private companies hosting content—including ISPs, cybercafes, and mobile phone operators—are obliged by law to hand over user information to the authorities. Prior judicial approval for communications interception is not required under either the Telegraph Act or the ITA, and the revised ITA grants both central and state governments the power to issue directives on interception, monitoring, and decryption.[67] Regulations passed in April 2011 increased monitoring requirements in cybercafes, requiring owners to obtain a copy of each user's photo ID and retain that record, as well as logs of all websites visited by the user, for one year.[68] The rules also contain specifications for the venue's layout, including placing limits on the height of cubicle partitions and requiring that certain monitors face the central area of the cybercafe.[69] Mobile phone operators are permitted to activate SIM cards only after users register their personal details with the carrier.

In January 2012, responding to a freedom of information request, the Home Ministry reported that the Central government orders 7,500 to 9,000 phone interceptions per

[65] "Professor arrested for poking fun at Mamata," Hindustan Times, April 13, 2012, http://www.hindustantimes.com/India-news/WestBengal/Professor-arrested-for-poking-fun-at-Mamata/Article1-839847.aspx.

[66] They were charged under Article 66 of the ITA, which appears to punish hacking offenses not online expression. See, Soudhriti Bhabani, "Professor held for uploading caricature of Mamata on social site," Daily Mail, April 13, 2012, http://www.dailymail.co.uk/indiahome/indianews/article-2129588/Professor-held-uploading-caricature-Mamata-social-site.html#ixzz246uKzJSf.

[67] The ITA's Section 69 expands the circumstances under which communications may be monitored, intercepted, and decrypted. Section 69B, for instance, allows the central government to collect traffic data from any computer source without a warrant, whether the data are in transit or in storage. See, "Yes, Snooping's Allowed," Indian Express, February 6, 2009, http://www.indi.anexpress.com/news/yes-snoopings-allowed/419978/0.

[68] Regulation reads: "When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorized for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing stating clearly the purpose of seeking such information or any such assistance."

[69] "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.

month.[70] Such activities have not been without controversy. Throughout 2011, media reports relayed accusations of intelligence and law enforcement agencies liberally engaging in phone and data interceptions, and in one case, two senior Mumbai police officers were found to have abused their ability to obtain user data in order to make a profit.[71]

Several court cases also highlighted both the government's and service providers' occasional sloppiness in handling requests for user information. Yahoo filed a case after the Controller of Certifying Authorities (CCA) had imposed a fine of 1.1 million Rupees (about US$22,000) when the company refused to hand over information related to about a dozen Yahoo IDs and IP addresses that the government said it suspected were being used by Islamic terrorists or Maoists. Yahoo refused the request, claiming it was not made through the channels required by law and argued in court that the CCA was not authorized to impose such a fine. In September 2011, the judge overturned the fine, but asked Yahoo to provide the information within one week.[72] In another long-running case, it emerged that Reliance Communications had tapped phone conversations of parliament member Amar Singh in 2005 based on a fraudulent letter allegedly from Delhi Police, despite the message being replete with grammar and spelling mistakes. In February 2011, the Supreme Court censured the government for not taking action against Reliance for its negligence.[73] These cases followed several scandals in 2009 and 2010 that revealed phone-tapping of lawmakers, politicians, and journalists.[74]

In recent years, the Indian authorities have reportedly enhanced their technical surveillance capabilities, but oversight has not always kept pace.[75] In December 2011, *The Hindu* newspaper reported on the proliferation and, in some cases misuse, of surveillance equipment purchased following the 2009 Mumbai terror attacks. The report alleged that the National Technical Research Organization had deployed monitoring equipment at key internet hubs, enabling large-scale surveillance of a particular area. Variants of such technologies then spread to police at the state level in places like Uttar Pradesh and

[70] Shyamlal Yadav, "9,000 orders for phone interception a month: Govt," Indian Express, January 23, 2012, http://www.indianexpress.com/news/9-000-orders-for-phone-interception-a-month-govt/902831/.
[71] "Two Delhi cops may land in the dock for selling cell call records," The Times of India, March 11, 2012, http://m.timesofindia.com/PDATOI/articleshow/12214794.cms.
[72] "Yahoo moves Delhi HC against govt," The Times of India, November 25, 2011, http://articles.timesofindia.indiatimes.com/2011-11-25/internet/30440468_1_internet-portal-web-portal-delhi-hc.
[73] "Supreme Court slams Centre over Amar Singh phone-tapping case," NDTV, February 12, 2011, http://www.ndtv.com/article/india/supreme-court-slams-centre-over-amar-singh-phone-tapping-case-84983.
[74] 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," Daily News & Analysis, December 16, 2010, http://www.dnaindia.com/india/report_government-mulling-law-to-regulate-phone-tapping_1481790.
[75] For example, three Indian firms were named in documents published by the anti-secrecy group Wikileaks as producing and selling sophisticated forms of surveillance equipment—including ones enabling speech analysis, location-tracking, and text-message monitoring. http://spyfiles.org/

Maharashtra. In an effort to reign in such activity, the federal Intelligence Bureau has reportedly tried to shut down 33 passive interception units, though with limited success. Meanwhile, officials in some states, like Andhra Pradesh, shut down such capabilities themselves after sensitive conversations among top officials were among the communications intercepted.[76] In November 2011, the authority to intercept phone calls, emails, and data communications domestically was extended to India's external intelligence agency, the Research and Analysis Wing, to facilitate the tracking of terrorist communications with individuals in foreign countries like Pakistan.[77] In March 2011, lawmaker Manish Tewari introduced a bill that would increase parliamentary oversight of intelligence agencies, but multiple stages of review remained before it might become law.[78] The executive branch has given little indication of intending to improve the legal framework surrounding surveillance activities.

Rather, India has emerged as a leader among countries urging telecommunications companies to reveal their codes or provide other ways for the authorities to intercept their traffic. The government threatened to shut down BlackBerry services in 2010, demanding that the device's manufacturer, Research in Motion (RIM), provide it with the capacity to read encrypted e-mail and instant messages sent via BlackBerry.[79] The dispute was partly resolved in 2011, as RIM established a facility in India to respond to government interception requests. Under the arrangement, the government can submit the name of a suspect it wants to wiretap and RIM will return decoded messages for that individual, provided it determines that the request was indeed lawful. Government officials have also reportedly expressed the desire to monitor communications transmitted over applications like Skype, Facebook, and Twitter more closely.[80]

India lacks a comprehensive privacy law and critics of the 2008 ITA amendments have raised concerns that the law did not adequately protect personal information held by corporations. However, the government has taken steps in recent years to improve the situation. In April 2011, the Indian parliament passed new, comprehensive data protection rules, which observers cited as comparable in some respects to European Union regulations. Though an

[76] Praveen Swami, "The government's listening to us," The Hindu, December 1, 2011, http://www.thehindu.com/news/national/article2678501.ece.
[77] "RAW gets power to tap phones, track emails," The Times of India, December 19, 2011, http://timesofindia.indiatimes.com/india/RAW-gets-power-to-tap-phones-track-emails/articleshow/11161977.cms.
[78] The Intelligence Services (Powers and Regulation) Bill, 2011, Bill No. 23 of 2011, 164.100.24.219/BillsTexts/LSBillTexts/asintroduced/7185LS.pdf.
[79] Bappa Majumdar, "BlackBerry Assures India on Access to Services," Reuters, August 13, 2010, http://www.reuters.com/article/idUSTRE67151F20100813; Mark Lee, "RIM Says BlackBerry Should Be Treated Equally as India Threatens Shut Down," Bloomberg, August 13, 2010, http://www.bloomberg.com/news/2010-08-13/rim-says-blackberry-should-be-treated-equally-as-india-threatens-shut-down.html.
[80] Amol Sharma, "RIM Facility Helps India in Surveillance Efforts," Wall Street Journal, October 28, 2011, http://online.wsj.com/article/SB10001424052970204505304577001592335138870.html#ixzz1itNw7Qq3.

improvement for privacy protection, the rules also drew criticism from the business community because they require immediate implementation (rather than having a transition period), do not allow online consent by users to suffice (written permission by fax, letter, or email is required), and were passed suddenly, quietly, and with little public consultation.[81] In early 2012, the Planning Commission went a step further, establishing a committee of experts to examine privacy laws in other countries and provide a detailed report on suggestions for a draft Privacy Bill for India.[82]

There have been no reports of government agents physically attacking bloggers or online activists. However, many online writers are cautious about what they post due to India's complex ethnic and religious make-up, occasional verbal intimidation, and concerns that online postings might spark communal violence, attacks from Maoists, or reprisals from religious extremists.

Several incidents occurred in 2011 highlighting the threat that hacking and cyber attacks could pose both for domestic and foreign affairs. In June 2011, intelligence agencies reported that a malicious virus was the suspected cause of technical problems at the Indira Gandhi International Airport that prompted the delay of dozens of flights.[83] Press reports in November 2011 indicated that the servers of India's National Informatics Centre had been compromised and used to launch attacks on other countries, including China, giving the impression that the attacker was the Indian government.[84] Meanwhile, loopholes in cyber security were exposed, as a reported 112 government websites were hacked between December 2011 and February 2012, including that of a state-owned telecom.[85]

[81] In August, the government clarified that firms in India's large outsourcing industry were exempt from the new rules. See, "Information Technology Act, 2000," Ministry of Communications and Information Technology; Miriam H. Wugmeister and Cynthia J. Rich, "India's New Privacy Regulations," Morrison & Foerster Client Alert. May 4, 2011, http://www.mofo.com/files/Uploads/Images/110504-Indias-New-Privacy-Regulations.pdf; Kochhar & Co, "2011 Indian Privacy Law," Outsourcing-Law.com, July 13, 2011, http://www.outsourcing-law.com/2011/07/2011-indian-privacy-law/; John Ribeiro, "India Exempts Its Outsourcers from New Privacy Rules," Network World, November 2, 2011, http://www.networkworld.com/news/2011/110211-india-exempts-its-outsourcers-from-252692.html.

[82] Vishwajoy Mukherjee, "New Bill to decide on individual's right to privacy," Tehelka, February 6, 2012, http://www.tehelka.com/story_main51.asp?filename=Ws060212Privacy.asp.

[83] Sidhartha Roy, "12-hour check-in failure at Terminal 3 caused by malicious virus attack?" Hindustan Times, July 5, 2011, http://www.hindustantimes.com/India-news/NewDelhi/12-hour-check-in-failure-at-Terminal-3-caused-by-malicious-virus-attack/Article1-717331.aspx.

[84] Josy Joseph, "Govt servers used for cyber attacks on China, other countries' networks," The Times of India, November 17, 2011, http://timesofindia.indiatimes.com/tech/news/internet/Govt-servers-used-for-cyber-attacks-on-China-other-countries-networks/articleshow/10760699.cms.

[85] John Ribeiro, "In India, 112 government websites hacked in three months," Network World, March 15, 2011, http://www.networkworld.com/news/2012/031512-in-india-112-government-websites-257311.html?hpg1=bn.

After details emerged on individuals from China infiltrating the Indian military and National Security Council,[86] indications surfaced that India was preparing an offensive cyber-warfare capability. According to press reports in August 2010, the government was considering a plan to enlist civilian professionals in efforts to hack the computer systems of hostile powers.[87] The reports of cyber-espionage from China also prompted fears that Chinese companies' growing stake in the telecommunications infrastructure market could facilitate future infiltration or sabotage.[88] In July 2010, the government issued regulations requiring equipment suppliers to allow the local operator, the government, or designated third-party agencies to "inspect the hardware, software, design, development, manufacturing facility and supply chain, and to subject all software to a security threat check."[89] The new rules have been met with significant objections from international companies, who warn that they exceed previous international practice.[90]

[86] "Shadows in the Cloud: Investigating Cyber Espionage 2.0," Information Warfare Monitor and Shadowserver Foundation, April 6, 2010, http://www.nartv.org/mirror/shadows-in-the-cloud.pdf.
[87] Harsimran Singh and Joji Thomas Philip, "Spy Game: India Readies Cyber Army to Hack Into Hostile Nations' Computer Systems," Economic Times, August 6, 2010, http://economictimes.indiatimes.com/news/news-by-industry/et-cetera/Spy-Game-India-readies-cyber-army-to-hack-into-hostile-nations-computer-systems/articleshow/6258977.cms.
[88] See, John Markoff and David Barboza, "Researchers Trace Data Theft to Intruders in China," New York Times, April 5, 2010, http://www.nytimes.com/2010/04/06/science/06cyber.html?_r=1; "Shadows in the Cloud: Investigating Cyber Espionage 2.0," Information Warfare Monitor and Shadowserver Foundation.
[89] Devidutta Tripathy, "Govt Tightens Telecom Rules on Security Concerns," Reuters, July 28, 2010, http://in.reuters.com/article/idINIndia-50466220100728.
[90] Erika Kinetz, "Tough Indian Telecom Rules Spark Foreign Backlash," R&D Magazine, August 3, 2010, http://www.rdmag.com/News/FeedsAP/2010/08/information-tech-tough-indian-telecom-rules-spark-foreign-backlash/.