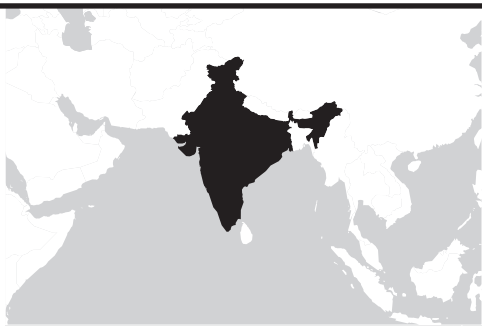
India



As a stable democracy with strong protections for press freedom, India's experiments with Internet filtering have been brought into the fold of public discourse. The selective censorship of Web sites and blogs since 2003, made even more disjointed by the non-uniform responses of Internet service providers (ISPs), has inspired a clamor of opposition. Clearly government regulation and implementation of filtering are still evolving.

Background

India is the world's second most populous nation, with a population of over one billion. India generally respects the right to free speech and the right to publish sensitive materials. A wide array of political, social, and economic beliefs is represented by the Indian media, generally without repercussion.[1] However, targeted censorship around issues of political and social conflict is a reality, particularly in areas of unrest. With the political turmoil present in the continuing dispute with Pakistan over Kashmir as well as fighting between religious groups, and issues between castes, the state takes an interest in censoring offensive material that could induce violence. Rarely are journalists detained on censorship issues, and they are often quickly released if held. Most violent attacks on journalists are carried out by religious or ethnic groups, with occasional harassment by state authorities.[2]

Internet in India

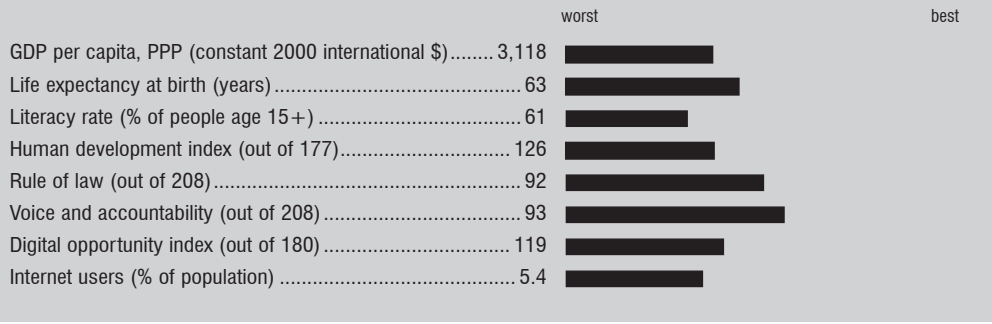
With an estimated forty-eight million users, the Internet community in India is the fifth largest in the world, although Internet users formed only about 4.3 percent of the country's population in 2005.[3] Access is gradually expanding from the most heavily populated urban centers, currently 41 percent of users, to small cities and towns.[4]

RESULTS AT A GLANCE

Filtering	No evidence of filtering	Suspected filtering	Selective filtering	Substantial filtering	Pervasive filtering
Political	●				
Social	●				
Conflict/security			●		
Internet tools			●		

Other factors	Low	Medium	High	Not applicable
Transparency			●	
Consistency		●		

KEY INDICATORS



Source (by indicator): World Bank 2005, 2006a, 2006a; UNDP 2006; World Bank 2006c, 2006c; ITU 2006, 2005

Because 71 percent of the population lives in rural areas, and because the gap between rural and urban teledensity is increasing, the majority of Indians are shut out of the Internet.[5] In decreasing order of popularity, points of access are cybercafés, home, work or business, and schools, with cybercafés remaining the most popular option.[6] An estimated 38 percent of all Internet users in India are "heavy users" and spend an average of 8.2 hours per week on the Internet.[7] A Windows Live Spaces report on a thriving blogging community in India, estimated at 14 percent of Internet users, found that a vast majority of bloggers are men under the age of thirty-five; this conforms to the demographic snapshot of Internet users as predominantly male, middle class, and young.[8]

There are 153 ISPs in operation today, although the majority market share (62 percent) remains with the public-sector corporations Bharat Sanchar Nigam Limited (BSNL) (43 percent) and Mahanagar Telephone Nigam Limited (MTNL) (19 percent).[9] In the mid-1980s two state-owned corporations were formed to provide limited telecom services—Videsh Sanchar Nigam Limited (VSNL) for international long distance, and Mahanagar Telephone Nigam Limited (MTNL) for Mumbai and Delhi. In 1995 VSNL was the first to provide Internet services in India, and it was privatized in 2002. The first Action Plan of the National Task Force on Information Technology and Software Development, created in May 1998, sought to create Internet access nodes in all district headquarters by January 2000. The government began allowing ISPs to legally handle Voice-over Internet Protocol (VoIP) in April 2002. As of March 2006, 134 ISPs were authorized to offer Internet-based telephony services, but only 32 were actually providing the service.[10]

In January 2007 the Department of Telecommunications (DOT) announced that it would be installing filtering mechanisms at India's international gateways. The head of the Internet Service Providers Association of India (ISPAI) stated that these new "landing stations" would be able to both engage in centralized filtering of Web sites and blocking of VoIP telephony services such as Yahoo, MSN, and Skype (and many more) that have not technically been approved to provide these services in India.[11]

Legal and regulatory frameworks

India guarantees freedom of speech and expression in its constitution, but reserves the authority to impose reasonable restrictions in the interests of the sovereignty and integrity of India, state security, foreign relations, public order, decency, or morality; or in relation to contempt of court, defamation, or incitement to an offense.[12] Each form of media—print, film, and television—is governed by its own regulatory apparatus. For example, the Press Council of India (PCI), a quasi-judicial body with two-thirds membership of representatives from print media, has a mandate to protect the independence of the press. The PCI adjudicates complaints against the media, issues normative guidelines, and performs a public education function.[13] In contrast, films cannot be exhibited without certification of a board appointed by the central government.[14] Private FM radio station ownership was legalized in 2000, but ownership licenses were granted only for stations airing entertainment or educational content; commercial and community FM radio stations are not allowed to broadcast news and current affairs.[15] The state still controls all AM radio stations.

Until the late 1990s, the Indian government had control over all aspects of the telecommunications sector—policy, regulation, and operations.[16] The New Internet Policy introduced in November 1998 allowed private companies to apply for licenses to become ISPs and either lease transmission network capacity or build their own, thereby ending the monopoly over domestic long distance networks of the Department of Telecoms. Most, however, opted to use the lines already established by the government.[17]

In June 2000 the Indian Parliament created the IT Act to provide a legal framework to regulate Internet use and commerce, including digital signatures, security, and hacking. The act criminalizes the publishing of obscene information electronically, and grants police powers to search any premises without a warrant and arrest individuals in violation of the act. [18]

The Indian Computer Emergency Response Team (CERT-IN) was set up by the Department of Information Technology under the IT Act to implement India's filtering regime.[19] By stretching the prohibition against publishing obscene content to include the filtering of Web sites, CERT-IN was empowered in 2003 to review complaints and act as the sole authority for issuing blocking instructions to the Department of Telecommunications (DOT).[20] Only specified individuals or institutions can make official complaints and recommendation for investigation to CERT-IN, a list that is limited to high-ranking government officials, the police, government agencies, and "any others as may be specified by the Government."[21] Many have argued that giving CERT-IN this power through executive order violates constitutional jurisprudence holding that specific legislation must be passed before the government can encroach on individual rights. The blocking mechanism created under the Act provides for no review or appeal procedures, except in court, and is permanent in nature. When CERT-IN has issued orders to block specific Web sites, no communication has been made to the public beforehand.[22]

Another basis for filtering was demonstrated with the blocking of the site www.hinduunity.org on April 28, 2004, reportedly ordered by the Mumbai police on the grounds that it contained inflammatory anti-Islamic material.[23] Police commissioners, who can exercise the powers of executive magistrates in times of emergency, can block Web sites containing material constituting a nuisance or threat to public safety under Section 144 of the Code of Criminal Procedure.[24] While major and small ISPs immediately complied with the blocking request, one of the nation's largests ISPs, Sify, refrained from blocking the Web site, arguing that only CERT-IN had the authority to issue blocking orders.[25]

Filtering can also be mandated through licensing requirements. For example, ISPs seeking licenses to provide Internet services with the DOT "shall block Internet sites and/or individual subscribers, as identified and directed by the Telecom Authority from time to time" in the interests of "national security."[26] License agreements also require ISPs to prevent the transmission of obscene or otherwise "objectionable material."[27]

The proposed amendment to the IT Act brought before Parliament on December 15, 2006, aims to address growing concerns about information security and data theft that threaten the vitality of India as an outsourcing hub.[28] Under specific conditions, the bill absolves intermediaries (including cybercafés) of responsibility for making available information or links created by third parties.[29] The government has also created "guidelines" for ISPs to follow, such as the monitoring of subscriber traffic by keyword and the disclosure of dynamic IP addresses of clients by ISPs.[30]

According to the Right to Information Act passed in 2005, designated government officers are required to respond to requests for information within thirty days.[31] Although it is not clear whether information about the blocking of Web sites falls within the exceptions listed in the Act,[32] which include information relating to national security and state sovereignty, individuals have filed RTI requests seeking greater transparency in the filtering process.[33]

ONI testing results

Results from ONI testing reveal that Indian ISPs selectively filter sites identified by government authorities as relating to national unity and state security. ONI conducted testing on Bharti, Direct, Reliance, YOU Telecom (formerly known as Iqara), Pacenet, and VSNL. Variations in blocking among ISPs of the same limited range of sites suggest that CERT-IN and the DOT continue to rely on ISPs to implement filtering instructions. Although obscene information is the only type of content to be made illegal under the IT Act, ONI found no evidence that pornography is filtered in India. Rather, nearly all the sites filtered had already been reported publicly as blocked at some time.

The only site made inaccessible by all ISPs tested was the Hindu Unity Web site (www.hindu unity.org), which was blocked as a result of an order from the Mumbai police using an alternative procedure to CERT-IN. (A number of different URLs direct to this site; these URLs were blocked with varying consistency between ISPs.) Further evidence that filtering has yet to be implemented through a uniform process can be found in the inconsistencies in filtering of the Web sites named in the CERT-IN blocking order following the bombings of suburban trains in Mumbai on July 11, 2006. On July 13, 2006, CERT-IN ordered access to seventeen Web sites blocked, reportedly because the attackers were believed to have communicated via the blogosphere. The Web sites that were ordered to be blocked included "American right-wing" sites (www.mypetjawa.mu.nu; www.mackers-world.com), Hindu extremist or "Hindutva" sites, and a defunct Web site supporting the formation of a "Dalit" homeland within India (www.dalitstan.org).[34]

Among the ISPs, Bharti, YOU Telecom, Reliance, and VSNL blocked the majority of sites included on the July 13 CERT-IN order. In this context, the personal Web site of a member of the Hindutva party VHP (and a university student in Indiana), www.rahulyadav.com, was filtered almost certainly because it was included in the July CERT-IN order, but the actual Web site of the VHP party (www.vhp.org) was available on all ISPs tested.

In 2006, filtering requests were also generated by individuals protesting content they considered offensive or obscene. In response to a Public Interest Litigation (PIL) petition calling for the ban of the social networking site Orkut for hosting a "We Hate India" community, the Bombay High Court had directed the Maharashtra government

to issue notice to Google for "alleged spread of hatred about India" on Orkut.[35] A month later, in response to protests over an "anti-Shivaji" community on Orkut, Pune police banned Orkut, temporarily shut down cybercafés where users were found to be using the site, and began an investigation under the IT Act and penal code provisions for obscene publications and religious insult.[36] In December 2006, a government official made a similar blocking request after reportedly "obscene" material about "Hindu girls" was posted on Orkut.[37] However, none of these efforts resulted in a comprehensive ban on Orkut, for though it was intermittently available in Pune it was nevertheless accessible on all ISPs tested.

ONI testing determined that filtering occurred at the ISP level, with considerable variation between ISPs. Direct, Pacenet, and VSNL blocked more of the tested URLs than did other ISPs. Filtering focused primarily on Web sites seen as a threat to national security, as well as sites offering untraceable communication such as the VoIP site www.hotfoon.com and the SMS gateway www.clickatell.com. Other sites, such as www.kahane.org, appear to have been blocked only because they shared an ISP address with a targeted site.

In contrast to the collateral blocking of Web sites in August 2003[38] and July 2006, where ISPs in both incidents responded to CERT-IN orders by cutting off access to parent Web sites including Google's www.blogspot.com, www.typepad.com, and Yahoo!'s www.geocities.com, banned Web site owners continue to migrate their content successfully to other domains. For example, while ISPs are clearly blocking on the subdomain level (for example, the site www.princesskimberley.blogspot.com is filtered on four ISPs tested), the reportedly banned Maoist Web site www.peoplesmarch.com was accessible in other forms (www.peoplesmarch.wordpress.com, www.naxalrevolution.blogspot.com) on all ISPs at time of testing.

Conclusion

Amidst widespread speculation in the media and blogosphere about the state of filtering in India, the sites actually blocked indicate that while the filtering system in place yields inconsistent results, it nevertheless continues to be aligned with and driven by government efforts. For example, efforts to block certain communities on Orkut, and in some instances the entire site altogether, have been initiated largely by individuals, but the government response has not resulted in the systematic blocking of Orkut by the ISPs that ONI tested. Government attempts at filtering have not been entirely effective, as blocked content has quickly migrated to other Web sites and users have found ways to circumvent filtering. The government has also been criticized for a poor understanding of the technical feasibility of censorship and for haphazardly choosing which Web sites to block. The amended IT Act, absolving intermediaries from being responsible for third-party created content, could signal stronger government monitoring in the future.

NOTES

1. U.S. Department of State, Country Reports on Human Rights Practices, 2006: India, http://www.state.gov/g/drl/rls/hrrpt/2006/78871.htm.
2. Ibid.
3. Paul Budde Communication Pty Ltd., India-Key Statistics and Telecommunications Market Overview, 2006, p. 2.
4. Internet and Mobile Association of India, Internet in India: 2006, http://www.iamai.in/research_index.php3.
5. Telecom Regulatory Authority of India, Indian Telecom Services Performance Indicators April-June 2006, October 2006, p. 40, http://www.trai.gov.in/Reports_content.asp?id=29.
6. Internet and Mobile Association of India, Internet in India: 2006, p. 16, http://www.iamai.in/research_index.php3.
7. Internet and Mobile Association of India, Internet in India-2006, p. 37, http://www.iamai.in/research_index.php3.
8. The Press Trust of India, "Indians prefer good-old diary to blogs," November 27, 2006.

9. Telecom Regulatory Authority of India (TRAI), Indian Telecom Services Performance Indicators April-June 2006, http://www.trai.gov.in/Reports_content.asp?id=29; http://www.indiabroadband.net/bsnl-broadband/2676-bsnl-top-isp-india.html.
10. TRAI Annual Report 2005–2006, http://www.trai.gov.in/traiannualreport.asp.
11. Indrajit Basu, "Security and censorship: India to clip the wings of Internet," January 16, 2007, Digital Communities, http://www.govtech.net/digitalcommunities/story.php?id=103332.
12. Article 19, The Constitution (Ninety-Third Amendment) Act, January 20, 2006, http://lawmin.nic.in/coi.htm.
13. Articles 13–15, Press Council Act 1978, http://presscouncil.nic.in/act.htm.
14. Parishi Sanjanwala, Internet Filtering in India, unpublished paper.
15. Ministry of Information and Broadcasting, Policy Guidelines for Setting up Community Radio Stations in India, http://mib.nic.in/welcome.html; Ministry of Information and Broadcasting, Grant of Permission Agreement, http://mib.nic.in/fm/fmmainpg.htm. See also Subramanian Vincent, "Community radio gets its day," India Together, November 18, 2006, http://www.indiatogether.org/2006/nov/sbv-cradio.htm.
16. See Thankom G. Arun, Regulation and competition: Emerging issues in an Indian perspective, Centre on Regulation and Competition, Working Paper Series No. 39, October 2003, www.competition-regulation.org.uk/publications/working_papers/wp39.pdf.
17. Peter Wolcott, The Provision of Internet Services in India, http://mosaic.unomaha.edu/India_2005.pdf.
18. The Information Technology Act, Article 67, 2000. Under the Act, anyone who publishes "any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt . . ." is subject to a fine and up to five years in prison. See http://www.sarai.net/journal/pdf/133-135%20(bill).pdf.
19. Notification no. GSR. 181(E), dated February 27, 2003; Notification GSR 529 (E) of July, 2003.
20. Ibid.
21. Notification no. GSR. 181(E) dated February 27, 2003, cited in Parishi Sanjanwala, Internet Filtering in India, p. 18.
22. Shivam Vij, "The discreet charms of the nanny state," National Highway, October 2006, at http://www.shivamvij.com/2006/10/the-discreet-charms-of-the-nanny-state.html.
23. Priya Ganapati, Mumbai Police Gag hinduunity.org, http://us.rediff.com/news/2004/may/26hindu.htm. See also Parishi Sanjanwala, Internet Filtering in India, p. 58.
24. Article 144, Code of Criminal Procedure, 1973, http://www.delhidistrictcourts.nic.in/CrPC.htm.
25. Priya Ganapati, Mumbai Police Gag hinduunity.org, http://us.rediff.com/news/2004/may/26hindu.htm (accessed May 23, 2006).
26. Schedule C, Section 1.10.2, Government of India, Ministry of Communications and Information Technology, Department of Telecommunications Telecom Commission, License Agreement for Provision of Internet Service (including Internet Telephony), http://www.dot.gov.in/ispt/isptindex.htm.
27. Schedule C, Section 1.12.9, Government of India, Ministry of Communications and Information Technology, Department of Telecommunications Telecom Commission, License Agreement for Provision of Internet Service (including Internet Telephony), http://www.dot.gov.in/ispt/isptindex.htm.
28. The Press Trust of India, "India to amend IT Act for greater data protection, privacy," October 16, 2006.
29. Article 79, The Information Technology (Amendment) Bill (2006), Bill 96 of 2006, http://www.mit.gov.in/.
30. See Ministry of Communications, Department of Telecom, Guidelines and General Information for Setting up of Submarine Cable Landing Stations for International Gateways for Internet, 2000, www.dot.gov.in/isp/landing_station.doc.
31. Article 7(1), Right to Information Act (2005), at http://www.righttoinformation.info/index.htm.
32. Article 8, Right to Information Act (2005), at http://www.righttoinformation.info/index.htm.
33. National Highway, "Internet censorship in India," http://www.shivamvij.com/2006/09/internet-censorship-in-india-an-rti-application.html.
34. A scanned copy of the July 13, 2006, CERT-IN order is available at http://photos1.blogger.com/blogger/507/157/1600/Indian_censored_list.jpg.
35. http://www.business-standard.com/general/printpage.php?autono=261383.
36. India Daily, "Orkut blocked in Pune, PIL filed against it for running anti Shivaji community," November 24, 2006, http://www.indiadaily.org/entry/orkut-blocked-in-pune-pil-filed-against-it-for-running-anti-shivaji-community/; Press Trust of India, "Orkut forum on Shivaji Maharaj blocked," November 18, 2006, http://www.expressindia.com/fullstory.php?newsid=77287.
37. Ganesh Kanate, "Patil wants bar on Orkut," DNA, December 9, 2006, http://www.dnaindia.com/report.asp?NewsID=1068353.
38. In August 2003, CERT-IN issued an order to ISPs to block the mailing list "kynhun" on Yahoo! Groups of the militant outfit Hynniewtrep National Liberation Council. See http://pib.nic.in/archieve/lreleng/lyr2003/rsep2003/22092003/r2209200314.html.