India

A stable democracy with a strong tradition of press freedom, India nevertheless continues its regime of Internet filtering. However, India's selective censorship of blogs and other content, often under the guise of security, has also been met with significant opposition.

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political			•		
Social			•		
Conflict and security			•		
Internet tools			•		

OTHER FACTORS

	Low	Medium	High	Not Applicable
Transparency		•		
Consistency			•	

KEY INDICATORS	
GDP per capita, PPP (constant 2005 international dollars)	2,970
Life expectancy at birth, total (years)	64
Literacy rate, adult total (percent of people age 15+)	nd
Human Development Index (out of 169)	119
Rule of Law (out of 5)	2.5
Voice and Accountability (out of 5)	3.0
Democracy Index (out of 167)	40 (Flawed democracy)
Digital Opportunity Index (out of 181)	124
Internet penetration rate (percentage of population)	5.1

Source by indicator: World Bank 2009, World Bank 2008a, World Bank 2008b, UNDP 2010, World Bank Worldwide Governance Indicators 2009, Economist Intelligence Unit 2010, ITU 2007, ITU 2009. nd, no data. See Introduction to the Country Profiles, pp. 222–223.

Background

With a population of over one billion, India is the world's second most populous nation. The Indian government, a constitutional republic and representative democracy, generally respects the right to free speech and allows a wide array of political, social, and economic beliefs to be expressed. However, on targeted political and social conflicts, the government censors media and online discussion, particularly in areas of social unrest. In conflicts between castes and religious groups, and in the ongoing dispute with Pakistan over Kashmir, the state routinely censors material it believes could incite violence. Threats to journalists and bloggers come from political, religious, or ethnic nationalist groups. However, journalists are rarely detained as a means of censoring the press, and when they are held they are often quickly released.

Internet in India

Internet use in India reveals a great imbalance between urban and rural regions, although the gap has been diminishing during the past few years. Nearly 25 percent of India's population lives in cities (266 million), and 20 percent (52 million) of those are active Internet users (meaning they have used the Internet at least once in the past month).[1] By contrast, only 4.18 million among the rural population are active users; 54 percent of these rural users access the Internet through Internet cafés more than ten kilometers away from their villages. Seventy-eight percent of nonusers

indicate that they are not aware of the Internet.[2] Language is another obstacle to using the Internet. Although there are 22 primary regional languages in India, most online content is in English, a language only 11 percent of the population speaks.[3] With approximately 61 million Internet users, India has an overall Internet penetration rate of 5.1 percent. However, its Internet subscription rate is low, at only 1.3 percent.[4]

Most Indians who access the Internet do so from Internet cafés. Home and work connections and school access points are less popular. Most Internet users in the country are male, middle-class, and young.[5] Almost half of the country's users are online at least four to six times per week.[6]

As of December 2009, approximately 370 Internet service providers (ISPs) were licensed to operate in the country.[7] According to an official Telecom Regulatory Authority of India report, Bharat Sanchar Nigam Limited (BSNL) and Mahanagar Telephone Nigam Limited (MTNL) were the market leaders, holding 57.84 percent and 13.81 percent of the market share respectively in June 2010.[8] 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 became the first to provide Internet services to the country. In April 2002, the government authorized ISPs to offer Voice over Internet protocol (VoIP) services.[9]

In January 2007, the Department of Telecommunications (DOT) announced that it would install filtering mechanisms at India's international gateways. The head of the Internet Service Providers Association of India (ISPAI) said that these new "landing stations" would be able to block both specific Web sites at the subdomain level and unauthorized VoIP telephone systems.[10]

Legal and Regulatory Frameworks

India guarantees freedom of speech and expression in its constitution but reserves the authority to impose restrictions in the interests of national sovereignty, state security, foreign relations, public order, decency, and morality.[11] Each form of media—print, film, and television—is governed by its own regulatory apparatus. For example, print media are regulated by a board of press and government officials,[12] while films are regulated by a board appointed wholly by the government.[13] Private FM radio stations were legalized in 2000, but none of them are allowed to broadcast news or current affairs. The state continues to retain control over all AM radio stations.[14]

Until the late 1990s, the Indian government had control over all aspects of the telecommunications sector: policy, regulation, and operations.[15] The new Internet policy introduced in November 1998 allowed private companies 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.

However, most companies opted to use the lines already established by the government.[16]

In June 2000, the Indian Parliament created the Information Technology Act (IT Act) to provide a legal framework to regulate Internet use and commerce, including digital signatures, security, and hacking. The act criminalizes publication of obscene information electronically and grants police powers to search any premises without a warrant and arrest individuals in violation of the act.[17]

In December 2008, the Indian Parliament amended the IT Act; the amended act came into force on October 27, 2009.[18] The 2000 IT Act had criminalized the electroinc publication of obscene information, granting police powers to search premises without warrants and arrest individuals in violation of the act.[19] The 2008 amendment broadened content that could be blocked beyond online obscenity. The newly added Section 69A grants power to the central government, "in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order," to issue directions to block public access to any information "generated, transmitted, received, stored or hosted in any computer resource."[20] Although Section 69A(2) requires procedures and safeguards to be prescribed when the government exercises this power,[21] these restrictions are unclear because they are not specified in the amendment. Critics claim that the amendment, which makes such sweeping changes in the existing regime, was passed "in an unprecedented hurry, without any discussion in both the houses of the Parliament."[22]

The Indian Computer Emergency Response Team (CERT-IN)[23] was set up by the Department of Information Technology under the amended IT Act to implement India's filtering regime.[24] In 2004, CERT-IN became operational to review complaints and act as the sole authority for issuing blocking instructions to the DOT.[25] Under the 2008 amendment of the IT Act, CERT-IN was assigned "the task of oversight of the Indian cyberspace for enhancing cyber protection, enabling security compliance and assurance in Government and critical sectors."[26] Only limited or specified individuals or institutions can make official complaints and recommendations for investigation to CERT-IN. These include high-ranking government officials, the police, government agencies, and "any others as may be specified by the Government."[27]

On July 13, 2006, CERT-IN ordered access to 17 Web sites blocked following the 2006 Mumbai train bombings, reportedly because the attackers were believed to have communicated by means of the blogosphere. The blocked Web sites included "American right-wing" sites (http://mypetjawa.mu.nu/, http://mackers-world.com/), Hindu extremist or "Hindutva" sites, and a defunct Web site supporting the formation of a "Dalit" homeland within India (http://www.dalitstan.org).[28]

In 2006, filtering requests also came from individuals protesting content they considered offensive or obscene. On October 10, 2006, media reported that the Bombay High

Court had directed the Maharashtra government to issue notice to Google for "alleged spread of hatred about India" on its social networking site Orkut, in response to a Public Interest Litigation (PIL) petition calling for the ban of Orkut for hosting a "We Hate India" community.[29] Similarly, in 2009, the Maharashtra government began examining legal options for censoring Google Earth, for fear that it could be used to facilitate terror attacks.[30] It was reported that the surviving gunman of the 2008 terror attacks in Mumbai claimed that Google satellite images had been used in planning the attacks.[31]

In November 2006, in response to protests over an "anti-Shivaji" community on Orkut, police banned Orkut, temporarily shut down Internet cafés where users were found using the site, and began an investigation under the IT Act and penal code provisions for obscene publications and religious insult offenses.[32] In December, a government official made a similar blocking request after a report that "obscene" material about "Hindu girls" was posted on Orkut.[33] In May 2007, although none of these efforts resulted in a comprehensive ban of Orkut, site officials reached an agreement with the Indian government to block "defamatory or inflammatory content" and to release the IP addresses of the offending parties to law enforcement.[34]

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. When CERT-IN has issued orders to block specific Web sites, no communication has been made to the public beforehand.[35] The blocking mechanism created under the IT Act provides for no review or appeal procedures, except in court, and is a permanent block.

Police commissioners, who can exercise the powers of executive magistrates in times of emergency, can also block Web sites containing material that constitutes a nuisance or threat to public safety under Section 155 of the Code of Criminal Procedure.[36] The first occurrence of such an action was in 2004, when Mumbai police blocked http://hinduunity.org on the grounds that it contained anti-Islamic material that could be inflammatory.[37] One of the nation's ISPs, Sify, refused to block the site on the basis that only CERT-IN had the authority to issue blocking orders.[38]

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."[39] License agreements also require ISPs to prevent the transmission of obscene or otherwise "objectionable material."[40]

Surveillance

Section 69 of the IT Act empowers the central government to designate agencies and issue orders for interception, monitoring, and decryption in the interest of national

security, public order, or preventing incitement of illegal acts. More specifically, Section 69B of the IT Act authorizes the central government to "monitor and collect traffic data or information through any computer resource for cyber security."[41] Within this authority, the law mandates that any intermediary or any person in charge of said computer resource called upon must "provide technical assistance and extend all facilities to such agency to enable online access," "intercept, monitor, or decrypt the information," and "provide information stored in computer resources."[42] Similar to Section 69A, the law requires that procedures and safeguards be applied when the government exercises such power, though the details of such procedures are not clear.

Concerned that terrorists may take advantage of the encryption in smart phones, the Indian government threatened to ban BlackBerry messaging and corporate e-mail services by August 31, 2010, unless Research in Motion (RIM) granted regulators access to encrypted user data. The deadline was first extended to October 2010, then to January 2011, for RIM and regulators to work on a feasible solution to address the national security concerns. As an interim solution, RIM agreed to host local servers and proposed a manual solution for messenger service.[43] In December 2010, India agreed to work with individual carriers to access data from BlackBerry devices, acknowledging RIM's assertion that they do not have access to individual users' encryption keys.[44]

According to Indian officials, the government also sent notices to Google and Skype, requiring them to set up local servers to allow full monitoring of encrypted e-mail and messenger communications.[45] It remains unclear how these service providers would comply with the direction.

ONI Testing Results

Results from OpenNet Initiative testing reveal that Indian ISPs selectively filter sites identified by government authorities. Over the course of 2009–2010, the ONI conducted testing on four major Indian ISPs: Bharti Airtel, Ltd.; Bharat Sanchar Nigam, Ltd. (BSNL); Tata Communications, Ltd.; and Mahanagar Telephone Nigam, Ltd. (MTNL). Testing done by the ONI found that BSNL blocked more Web sites than the other ISPs, which had only slight variations among them. Variations in blocking among ISPs suggest that CERT-IN and the DOT continue to rely on ISPs to implement filtering instructions.

When users attempt to access a blocked Web site on any of the four tested ISPs, they receive a "server not found" error page. This error page—also received in the instance of a genuine server error—gives users the impression that the Web sites are inaccessible as a result of routine network errors, rather than filtering.

OpenNet Initiative technical analysis revealed that these errors were the result of DNS tampering, a method of filtering that enables ISPs to target specific content. As a result, ISPs are able to block individual blogs (such as http://pajamaeditors.blogspot.com, http://commonfolkcommonsense.blogspot.com, and http://exposingtheleft

.blogspot.com) without blocking the host domain, http://blogspot.com, or any of the other blogs hosted on it.

While BSNL blocked more sites than the other ISPs, the ONI found that in general the level of filtering among ISPs was consistent with only slight variations. Further, the contents of filtered Web sites are similar across ISPs. For example, each ISP blocks a variety of extremist sites, such as Web sites of Hindu extremist groups (http://hinduunity.com and http://hinduunity.org) or Web sites with critical or extremist political (particularly "American right-wing") commentary (http://mypetjawa.mu.nu, http://mackers-world.com/). The OpenNet Initiative has found that these sites are consistently targeted for filtering by India. Web sites with information on human rights in India, Internet tools such as proxies, and content related to free expression are also targets of filtering. Data also showed that ISPs consistently filter pornography, but compared to other types of content, the number of blocked pornographic sites is small.

Technical analysis revealed evidence of collateral filtering on two ISPs: Bharti Airtel and MTNL. Collateral filtering is a result of IP-based blocking and refers to Web sites that are unintentionally filtered as a result of sharing the same IP address as a Web site that has been intentionally blocked. For example, 2006–2007 testing found that a site about American-Israeli rabbi Meir Kahane (http://kahane.org) was blocked because it shares the same IP address as the Hindu Unity Web site (http://hinduunity.com, http://hinduunity.org); 2009–2010 testing confirmed that the block was still in place. Similarly, during 2008–2009 testing a Web site for travel agents (http://www.positivespace.com) and a system administrator resource Web site (http://gwsystems.co.il) were found blocked as a result of sharing that same IP address with the Hindu Unity Web site.

Conclusion

Indian ISPs continue to selectively filter Web sites identified by authorities. However, government attempts at filtering have not been entirely effective because 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. There are still parts of the IT (Amendment) Act, including absolving intermediaries from being responsible for third-party-created content, that have not been tested since its enactment. This lack of action could signal stronger government monitoring in the future.

Notes

1. Internet and Mobile Association of India (IAMAI), "I-Cube 2009–2010: Internet in India," April 2010, http://www.iamai.in/Upload/Research/icube_new_curve_lowres_39.pdf.

2. IAMAI, "Internet for Rural India: 2009," August 2010, http://www.iamai.in/Upload/Research/Internet_for_Rural_India_44.pdf.

3. IAMAI, "I-Cube 2009–2010: Internet in India."

4. International Telecommunication Union (ITU), "Internet Indicators: Subscribers, Users and Broadband Subscribers," 2009 Figures, http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False.

5. IAMAI, "I-Cube 2009–2010: Internet in India."

6. Ibid.

7. Department of Telecommunications, Ministry of Information and Technology India, "List of ISP Licensees as on 31.12.2009," December 31, 2009, http://www.dot.gov.in/isp/ISP_licences_31.12.09.doc.

8. Telecom Regulatory Authority of India, "Indian Telecom Services Performance Indicators April-June 2010," October 2010, http://www.trai.gov.in/WriteReadData/trai/upload/Reports/52/5octoblerindicatorreporton13oct.pdf.

9. Rakesh Kumar Sharma and R. K. Yadav, "Reforms in Indian Telecom Sector," Indian MBA, http://www.indianmba.com/Faculty_Column/FC701/fc701.html.

10. Joji Thomas Philip and Moumita Bakshi Chatterjee, "Screening for Dangerous Blogs, Sites," *India Times Infotech*, December 5, 2006, http://www.digitalcommunities.com/articles/Security-and-Censorship-India-to-Clip.html.

11. Constitution Act of India (Ninety-Third Amendment), Article 19, http://lawmin.nic.in/coi.htm.

12. Indrajit Basu, "Security and Censorship: India to Clip the Wings of Internet," Digital Communities, January 26, 2007, http://www.digitalcommunities.com/articles/Security-and-Censorship-India-to-Clip.html.

13. Constitution Act of India (Ninety-Third Amendment), Article 19.

14. Press Council Act 1978, Articles 13–15, http://presscouncil.nic.in/act.htm.

15. Thankom G. Arun, "Regulation and Competition: Emerging Issues in an Indian Perspective," Centre on Regulation and Competition, October 2003, http://www.competition-regulation.org.uk/publications/working_papers/wp39.pdf.

16. Policy Guidelines for Setting up Community Radio Stations in India, Ministry of Information and Broadcasting, http://www.mib.nic.in/writereaddata/html_en_files/crs/CRBGUIDELINES041206.pdf; Subramanian Vincent, "Community Radio Gets Its Day," India Together, November 18, 2006, http://www.indiatogether.org/2006/nov/sbv-cradio.htm.

17. Information Technology (IT) Act 2000, Ministry of Information Technology, http://www.mit.gov.in/content/view-it-act-2000.

18. Enforcement of Information Technology (Amendment) Act 2008, Department of Information Technology, http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/act301009.pdf.

19. IT Act, 2000, Article 67.

20. IT Act, 2008.

21. Ibid.

22. Comments by Pavan Duggal, President of Cyberlaws.net, http://www.cyberlaws.net/itamendments/index1.htm.

23. Indian Computer Emergency Response Team, http://www.cert-in.org.in.

24. Right to Information Act, 2005, Article 7(1), http://righttoinformation.gov.in/webactrti.htm.

25. Shivan Viv, "Internet Censorship in India: An RTI Application," National Highway, September 26, 2006, http://shivamvij.com/2006/09/26/internet-censorship-in-india-an-rti-application.

26. Vikas Asawat, "Information Technology (Amendment) Act, 2008: A New Vision through a New Change," March 17, 2010, http://ssrn.com/abstract=1680152.

27. Department of Telecommunications, Ministry of Communication and Information Technology, "Directions to Block Internet Websites," http://photos1.blogger.com/blogger/507/157/1600/Indian_censored_list.jpg.

28. Right to Information Act, 2005, Article 7(1).

29. Ibid., Article 8.

30. "Maharashtra Wants Google Earth Censored," *The Hindu*, March 10, 2009, http://www.hindu.com/holnus/004200903101511.htm.

31. "India's Own Version of Google Earth Causes Security Worries," *Economic Times*, March 11, 2009, http://economictimes.indiatimes.com/Infotech/Indias-own-version-of-Google-Earth-causes-security-worries-/articleshow/4250421.cms.

32. Viv, "Internet Censorship in India."

33. Department of Telecom, Ministry of Communication and Information Technology, "Directions to Block Internet Websites."

34. "Orkut's Tell-All Pact with Cops," *Economic Times*, May 1, 2007, http://articles.economictimes.indiatimes.com/2007-05-01/news/28459689_1_orkut-ip-addresses-mumbai-police.

35. John Ribeiro, "Orkut Comes under Fire in India," *InfoWorld*, October 12, 2006, http://www.infoworld.com/t/architecture/orkut-comes-under-fire-in-india-310.

36. Chinmayee Prasad, "Analysing Section 144, CrPC," National Law Institute University Bhopal, http://www.legalservicesindia.com/articles/crpc.htm.

37. Pratyush, "Orkut Blocked in Pune, PIL Filed against It for Running Anti Shivaji Community," India Daily, November 24, 2006, http://pratyush.instablogs.com/entry/orkut-blocked-in-pune-pil-filed-against-it-for-running-anti-shivaji-community/; "Orkut Forum on Shivaji Maharaj Blocked," Press Trust of India, November 18, 2006, http://www.expressindia.com/news/fullstory.php?newsid=77287.

38. Ministry of Communications and Information Technology, "Blocking of Website," September 22, 2003, http://pib.nic.in/archieve/lreleng/lyr2003/rsep2003/22092003/r22092003314.html.

39. Code of Criminal Procedure, 1973, Article 144, http://www.delhidistrictcourts.nic.in/CrPC.htm.

40. Priya Ganapati, "Mumbai Police Gag hinduunity.org," Rediff, May 27, 2004, http://ia.rediff.com/news/2004/may/26hindu.htm.

41. Information Technology (Amendment) Act 2008, http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf.

42. Ibid.

43. Shauvik Ghosh, "Govt Gives RIM Time till Jan to Provide Data Access," October 12, 2010, Livemint, http://www.livemint.com/2010/10/11235823/Govt-gives-RIM-time-till-Jan-t.html.

44. Nancy Gohring, "RIM: India Agrees to Work with Enterprises for Data Access," *PC World,* December 3, 2010, http://www.pcworld.com/businesscenter/article/212462/rim_india_agrees_to_work_with_enterprises_for_data_access.html.

45. Devidutta Tripathy, "India to Decide on More Time to RIM for Data Access," Reuters, October 26, 2010, http://www.reuters.com/article/2010/10/26/india-rim-idUSSGE69P0IU20101026.

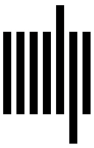
Access Contested

Security, Identity, and Resistance in Asian Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Contested: Security, Identity, and Resistance in Asian Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/9780262016780.001.0001
ISBN (electronic): 9780262298919
Publisher: The MIT Press
Published: 2011



The MIT Press

The online edition of this work is available from IDRC and at http://www.access-contested.net.

International Development Research Centre
PO Box 8500, Ottawa, ON K1G 3H9, Canada
info@idrc.ca / www.idrc.ca <http://www.idrc.ca>
ISBN 978-1-55250-507-6 (IDRC e-book)

This book was set in Stone Sans and Stone Serif by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access contested : security, identity, and resistance in Asian cyberspace / edited by Ronald Deibert . . . [et al.].
p. cm. — (Information revolution and global politics)
Includes bibliographical references and index.
ISBN 978-0-262-01678-0 (hardcover : alk. paper) — ISBN 978-0-262-51680-8 (pbk. : alk. paper)
1. Cyberspace—Government policy—Asia. 2. Computer security—Asia. 3. Computers—Access control—Asia. 4. Internet—Government policy—Asia. 5. Internet—Censorship—Asia. I. Deibert, Ronald.
HM851.A253 2011
303.48′33095—dc23

2011031273

10 9 8 7 6 5 4 3 2 1