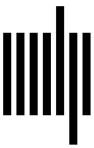
Access Denied

The Practice and Policy of Global Internet Filtering

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

Citation:

Access Denied: The Practice and Policy of Global Internet Filtering
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/7617.001.0001
ISBN (electronic): 9780262255998
Publisher: The MIT Press
Published: 2008



The MIT Press

Internet Filtering in **Asia**

Overview

It is not surprising that Asia, a region with extraordinary cultural, social, and political diversity, is home to a broad range of approaches, policies, and practices toward Internet censorship.

ONI conducted in-country testing in Afghanistan, China, India, Malaysia, Myanmar (Burma), Nepal, Pakistan, Singapore, South Korea, Thailand, and Vietnam. Afghanistan, Malaysia, and Nepal do not use technical filtering to implement their policies on information control, but China, Myanmar, and Vietnam rely heavily on pervasive filtering as a central platform for shaping public knowledge, participation, and expression. The filtering practices of Thailand and Pakistan are more targeted, as ONI testing indicated that they blocked a substantial number of sites across categories of content considered sensitive or illicit. The remaining countries in Asia tested by ONI filtered on a selective basis and on targeted topics, including India (ethnic and religious conflict), South Korea (sites containing North Korean propaganda or promoting the reunification of North and South Korea), and Singapore (pornography).

Of countries filtering political content, China, Myanmar, and Vietnam blocked with the greatest breadth and depth, spanning human rights issues, reform and opposition activities, independent media and news, and discrimination against ethnic and religious minorities. Thailand and Pakistan blocked political content to a much more limited degree than China, Myanmar, or Vietnam.

A narrower range of social content was blocked in Asian countries. Many countries, including Vietnam, cited obscene content as a major justification for engaging in technical filtering. Singapore, Thailand, China, Pakistan, and Myanmar actually blocked pornographic content to varying degrees. Pakistan filtered a number of sites posting Danish cartoon images of the Prophet Muhammad widely condemned as blasphemous, while India also blocked a limited number of sites providing extreme viewpoints on religion. South Korea and Thailand filtered a small selection of gambling sites.

Conflict and security blocking was carried out by Myanmar, China, South Korea, India, Pakistan, and Thailand most frequently in regard to groups or movements implicated in "secessionist" or pro-independence activities, or in regard to disputed territories and border conflicts.

Myanmar, China, Vietnam, Thailand, and Singapore filtered Internet tools, including free Web-based e-mail providers, blog hosting services, and more frequently proxies and other circumvention tools. South Korea blocked pirated software on a nominal basis.

Internet in Asia

Some of the most and least connected countries in the world are located in Asia: Japan, South Korea, and Singapore all have Internet penetration rates of over 65 percent, while Afghanistan, Myanmar, and Nepal remain three of thirty countries with less than 1 percent of its citizens online.[1]

Among the countries in the world with the most restricted access, North Korea allows only a small community of elites and foreigners online. Most users must rely on Chinese service providers for connectivity, while the limited number of North Korean–sponsored Web sites are hosted abroad.

Even with an Internet penetration rate of only 10 percent, China was host to 137 million Internet users at the end of 2006.[2] The Chinese government predicted that within two years China would overtake the United States in becoming the country with the greatest number of Internet users worldwide.[3] Similarly, though India's Internet community is the fifth largest in the world, users amounted to only about 4 percent of the country's population in 2005.[4]

Afghanistan, Myanmar, and Nepal are among the world's least-developed countries. Despite the constraints on resources and serious developmental and political challenges, however, citizens are showing steadily increasing demand for Internet services such as Voice-over Internet Protocol (VoIP), blogging, and chat. The Internet market in Nepal is growing rapidly as a result of a competitive Internet service provider (ISP) market and low Internet access prices.[5] In Afghanistan, the Internet and information communications technology (ICT) have been identified as important sources of growth and development, with the potential to create opportunities for disadvantaged groups such as women, whose literacy rate stands at least 10 percent lower than the overall adult literacy rate of 28 percent. [6]

The range in access to broadband and high-speed Internet in Asia on a national basis is also staggering. South Korea has the highest rate of Internet penetration in the world: more than 89 percent of South Korean households had Internet access, and 75 percent of them used broadband in 2005.[7] As a result of heavy investment in its broadband infrastructure following the Asian financial crisis in the late 1990s, South Korea provides its citizens with a national network that carries data at speeds up to 50 Mb/s.[8] In 2005 the number of Internet users in Singapore reached 2.42 million, or 67 percent of the population,[9] one of the highest Internet penetration rates in the world. Singapore became the "first fully connected country in the world" by acting on a commonly held belief that the integration of technology is essential to achieving economic growth.[10] Home access is commonplace, with residential dialup and broadband subscriptions totaling more than 2.1 million.[11] Although Thailand has a penetration rate of 19 percent, homes and businesses in Bangkok and other major cities account for most of the connectivity;[12] only around 15 percent of schools in 2004 had access the Internet, and broadband access for households is at less than 2 percent penetration.[13] In Pakistan, broadband and high-speed Internet is accessible only to wealthier individuals or businesses: the majority of home Internet users are connected by modem, while cybercafés tend to split one modem or DSL connection over many computers, reducing connection speed.

Regional, language, and ethnic differences also impact access to Internet services and ICT infrastructure, and frequently reflect other disparities in national development priorities and resource allocation. China's longstanding policy of extracting taxes and other resources from rural areas to fund coastal development has resulted not only in alarming rural-urban income disparities, but also has contributed to a growing digital divide: while a quarter or more of residents in major cities such as Tianjin are online, in poorer and western provinces the rate is usually less than 10 percent.[14] Access in India is gradually expanding from the eight most heavily populated urban centers, where 41 percent of users are concentrated, to small cities and towns.[15] Since 71 percent of the population lives in rural areas, and since the gap between rural and urban teledensity is increasing, the majority of Indians are shut out of the Internet.[16] In Thailand and Vietnam it is believed that Internet use will increase as content (including search engines) becomes available in local languages rather than English.

User-generated content and media, which has ballooned in the scale and the scope of its influence, continued to shape—and in many cases redefine—the dissemination and generation of information in many Asian countries. In media climates where news publications are frequently owned by the state or controlled by business interests with close ties to ruling parties, bloggers and other independent content providers are becoming an increasingly trusted source of news, and in many cases have broken stories that are picked up by mainstream media. At the same time, the popularity of blogs and portals discussing political issues and reform in countries such as Malaysia and China indicate that citizen-generated content is filling an important information deficit in highly controlled media environments.

For example, despite the government's requirement that "persistently" political blogs and Web sites would be required to register and then abstain from engaging in election campaigning in the run-up to the 2006 general elections in Singapore, "citizen media" uploaded footage of opposition party rallies taken with handheld video cameras and cell phones to media-sharing sites such as YouTube and Google Video. This participation marks a departure from perceptions that the vast majority of Singaporeans "do not consider the Internet to [sic] useful for political engagement and civic participation."[17] Although very few Nepalis have access to the Internet, it has nevertheless become an important source of independent news in Nepal.[18] When King Gyanendra assumed authoritarian control in 2005, Nepali bloggers became an important political voice and source of information to the world about the situation unfolding inside the country, as traditional media were either shut down or heavily censored.[19] In a study of MSN users in Hong Kong, India, Malaysia, Singapore, South Korea, Taiwan, and Thailand, 41 percent of bloggers were "active" (spending three hours or more each week blogging), and with the exceptions of India and South Korea, a majority of bloggers in these countries were women.[20] Online citizens' media has played an important role in South Korean politics and Internet culture in recent years, led by ohmynews.com, a Seoul-based online newspaper that publishes articles mostly written by 50,000 citizen journalists and is considered the most influential news source in South Korea.[21] OhmyNews has been widely acknowledged as strongly influencing the 2002 election of Korean President Roh Moo-hyun.[22]

Age is an essential demographic factor to consider when tracking trends in Internet use and growth in Asia. In Vietnam—which has an Internet penetration rate of 17 percent, where more than half of the population is under thirty, and where a significant portion of individual users use cybercafés for online gaming and access to the Internet—control over these venues is an important priority for the state.[23] In China, eighteen- to twenty-four-year-olds comprise over 35 percent

of all Internet users.[24] Over 70 percent of the 20.8 million bloggers (of which around 3.15 million were active) are under thirty.[25] In Thailand those under twenty-five years account for over half of Thai users.[26] 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, which conforms to the demographic snapshot of Indian Internet users as predominantly male, middle class, and young.[27]

Legal and regulatory frameworks

Each of the countries that practice pervasive filtering in the region have issued ambitious regulations that aim to bring Internet users under government supervision and control, even if the feasibility of such oversight remains in doubt. Myanmar, China, and Vietnam engage in constant, unremitting supervision of and interference with other forms of media. Well-established strategies include the shuttering of reformist newspapers and Web sites, the institutionalized supervision over content, and the intimidation and harassment of dissidents, journalists, and human rights activists.

In the regulation of cyberspace, the corresponding phenomenon is the delegation of policing and monitoring responsibilities to ISPs, content providers, private corporations, and users themselves. These frameworks are not structured to accommodate only voluntary self-regulation along industry lines, but rather they exact compliance with state-imposed requirements through the looming threat of shutdowns, loss of license, fines, job dismissals, and even criminal liability. Vietnam and China apply a more direct form of censorship through the detention of cyberdissidents, while in Pakistan the Supreme Court authorized the police to register criminal cases against publishers of content blaspheming the Prophet Muhammad, even though no one was apprehended. Although there are no known cases of individuals detained for merely viewing prohibited online content, there are scores of journalists, writers, and activists who have been imprisoned on the basis of publishing criticism of government policies on the Internet, even in the form of song lyrics or discussion of political reform over VoIP.[28] The hidden, cumulative cost of these tiered and overlapping controls is self-censorship and a chilling effect that pervades all speech.

China can point to dozens of regulations that systematically proscribe nine to eleven types of illegal content, and the number of regulations is growing. The government has imposed new regulations to keep pace with, and even anticipate, the explosion of online video sharing, blogging, and other Web 2.0 platforms, proposing real-name registration requirements for bloggers and national regulations for online video and short film content.[29] With the support of a legal framework where even unemployment rates and certain family planning statistics are state secrets, the central propaganda organ issues instructions throughout the government hierarchy to media organizations, hosts such as BBS and blog platforms, and other content providers to suppress discussion of an ever-expanding list of proscribed topics.

Whether or not a legal basis for filtering is implicit in content regulations, in many Asian countries filtering has proceeded despite the lack of clear authority to do so. This includes countries with established democratic systems and protections for the press and other forms of speech. For example, while India is in the process of centralizing its filtering at the international gateway level and therefore improving its efficacy, many still question whether its primary legal authorization for filtering, the 2000 IT Act, is valid in light of constitutional requirements for limits to freedom of expression.

In Thailand, where human rights protections and press freedom have deteriorated in recent years, the legal authority for filtering is not clear. Indeed, the practice of filtering may in fact con-

tradict protections in the 1997 Constitution that guarantee Thai citizens the rights to express opinions, to communicate by "lawful" means, and to access information.[30] The first military coup in fifteen years, in September 2006, amplified the uncertainty over the legitimacy of government policy, particularly through the declaration of martial law that precipitated claims of increased filtering.[31] The new military government took controversial and unilateral measures such as abrogating the Thai Constitution and banning new political parties, but ONI testing revealed that the post-coup content targeted for filtering was generally continuous with the filtering regime established by former Prime Minister Thaksin Shinawatra's government.

Defamation laws

A popular tool for silencing critics in countries such as Singapore, Malaysia and China, defamation laws and other forms of civil and criminal liability have begun to be applied to compel independent news sources, bloggers, and others to remove or retract online content.

In Singapore, defamation suits levy civil liability and heavy damages on independent and critical voices, from opposition party politicians to regional publications with domestic circulation.[32] Thai journalists and other critics of former Prime Minister Thaksin Shinawatra's ruling party had been similarly targeted, in line with a well-established precedent for using defamation suits to silence those fighting corruption.[33] Individuals perceived as criticizing the King, an act of lèse majesté, can be found liable under both defamation laws and the criminal code. In Malaysia, the first defamation suits against bloggers were inaugurated in January 2007, where the *New Straits Times* paper and several of its executives sued Jeff Ooi (www.jeffooi.com) and Ahirudin Attan (www.rockybru.blogspot.com) simultaneously for both blog posts and reader comments critical of their coverage.[34]

Implementation of filtering

However, even where legal authority for technical filtering and other forms of Internet censorship has been clearly established, filtering remains a contested practice.

At times an important source of conflict between users and government is the clumsy execution of imprecise methods, leading to a much broader scope of filtering than what was authorized. This was the case in Pakistan in February 2006, where a strong public outcry to "blasphemous" Danish cartoons depicting the Prophet Muhammad contributed to the blocking of twelve sites posting the images. The initial blockage quickly mushroomed into a mandate to filter all blasphemous content and resulted in the collateral blocking of the Blogspot domain for most of 2006, a consequence of the use of IP blocking. In India, the collateral blocking of Web sites occurred in response to CERT-IN orders in August 2003 and July 2006,[35] where ISPs in both incidents cut off access to parent Web sites including Google's blogspot.com, typepad.com, and Yahoo!'s geocities.com. One exception to the elastic filtering frequently encountered in Asian countries is North Korea, where access to online content is limited to the few dozen Web sites in Kwangmyong, the nation's domestic intranet.

In the implementation of technical filtering, the content blocked also frequently departs from pre-established or publicly acknowledged targets. For example, despite its putative focus on cleansing the Web of "harmful" social content such as obscenity,[36] the South Korean government uses its authority to define "harmful" content to focus on pro-North Korean or pro-reunification material. ONI testing found very little blocking of sensitive social content. The variations in filtering, if not the type of content blocked, between the two state-owned ISPs in Myanmar were surprising given the government's lockdown on information and all forms of media. India's IT Act, cited as the authority for the cre-

ation of the filtering certification body CERT-IN, prohibits only the publication of obscene content; however, CERT-IN has used its authority to issue blocking instructions against religious and ethnic inflammatory content.

Nonstate actors—especially ISPs—are deputized not only to shoulder monitoring duties and legal responsibility for unauthorized online behavior, but in many Asian countries they are relied upon to implement technical filtering. Countries that filter effectively at the international gateway were the exception in Asia. The two main state-owned ISPs in China each control a backbone network, and filtering was remarkably consistent between them. Blocking between South Korean ISPs was extremely consistent, even though both Korea Telecom (KorNet) and Hanaro Telecom (HanaNet) are publicly held corporations. In most other countries, the implementation of filtering primarily at the "margins" of state action has led to significant disparities across ISPs (especially in a crowded market), potential overblocking, and other inconsistencies such that users in the same country experience their "right" to access information differently and are able ultimately to view and interact with different portions of the Internet.

Additionally, the scope of a state's legal regulation of online activity often belies an implementation of state policy that is not entirely monolithic. Myanmar, China, Vietnam, India, and Pakistan all have regulations requiring cybercafés to monitor the online activities of their users and demand personal identity information. Generally these policies are difficult to enforce. For example, though the Myanmar government requires that users be registered and that screenshots of their activity be taken every five minutes, cafés do not always comply and CDs of screenshots are requested only sporadically.[37]

Impact of economic and social factors

Economic incentives and social factors have a definite impact on filtering practices in Asia. Global industry players such as Google and Microsoft have engaged in censorship in order to benefit from state investment in providing improved speed and quality of access to approved content while strengthening technical filtering, particularly in China.

On June 29, 2006, India's Department of Telecommunications (DOT) reportedly instructed around 150 ISPs to block the Web site of the People's War Group (PWG), a Maoist paramilitary group that was hosted on Geocities. A month later, the DOT informed ISPs that Yahoo! had removed the PWG's site, apparently the first time a service provider had voluntarily removed a Web site to avoid being blocked.[38]

The Chinese and Vietnamese governments must contend with the challenge of maintaining control over specified corridors of information as the space for approved or harmless topics grows increasingly vast. Myanmar has taken a blunter approach than its authoritarian neighbors, and in the case of China, its stalwart ally and aid provider. Internet access in Myanmar is structured so that broadband costs are prohibitive for most of its citizens, and dialup access comes bundled with state-monitored, fee-based e-mail service and a small collection of pre-approved sites on the country's intranet. In a reported attempt to not only censor communications but also preserve its monopoly over telephone and e-mail services as MPT's revenues dipped, the government blocked free e-mail services at points in 2006.[39] ONI testing confirmed that Yahoo! Mail, Gmail, Hushmail, and mail2web were blocked, with the ISP Myanmar Posts and Telecom taking the additional precaution of blocking thirteen additional e-mail sites, including Hotmail and Fastmail. Similar concerns about loss of state revenue have factored into similar tightening of VoIP services in Pakistan and China.

Economic motivations may also work to achieve an opposite effect, where governments explicitly refrain from Internet censorship in order to encourage growth. A number of Asian coun-

tries known for effective and sophisticated systems of information control, such as Singapore and Malaysia, demonstrated surprisingly low levels of filtering. For these governments, the strength of their historical interventions in freedom of the press and free speech may partially obviate the need for rigorous filtering.

In contrast to its approach toward other forms of media, the official policy of Singapore's Media Development Authority (MDA) has been to apply a "light-touch" regulatory framework to the Internet, promoting responsible use while giving industry players "maximum flexibility." Thus Singapore filters content on a symbolic scale, but also relies on established controls over print and broadcast media to set a precedent for citizens' online behavior, leading one scholar to call media regulation a "dual regulatory regime."[40] Greater control of cyberspace may be obviated by existing restrictive laws, political ties to the judiciary, and ownership and intimidation of the media that are already used to suppress dissenting opinion and opposition to the ruling People's Action Party (PAP).[41] Taken together, these economic and legal controls contribute to a climate of pervasive self-censorship of political commentary.

In Malaysia the state pledges not to censor Internet content in its "Bill of Guarantees" to companies approved for its Multimedia Super Corridor (MSC), a high-tech business center and communications infrastructure designed to help the country become an international information technology leader.[42] However, rather than filter content, Malaysia's Communications and Multimedia Act (CMA) targets "indecent" and "offensive" online content by subjecting publishers and authors to civil and/or criminal liability. Internet content publishers in Malaysia operate under the constant risk that the CMA and numerous other laws regulating speech and content on traditional media will be interpreted or amended to extend to Internet publications.[43] Notably, the bloggers Jeff Ooi and Ahirudin Attan were targeted under defamation laws and not the regulatory framework for online speech, which delineates fines and criminal penalties for persons using a content applications service to provide content that is "indecent, obscene, false, menacing, or offensive in character."[44]

In Afghanistan and Nepal serious political and economic challenges have perhaps made technical filtering impracticable, but this does not mean their citizens have unfettered access to information and communication via the Internet. Political instability has affected not merely the quality of access, but also the question of access altogether. The Internet in Afghanistan was banned altogether by the Taliban in July 2001—primarily because it was thought to broadcast obscene, immoral, and anti-Islam material, and the few Internet users at the time could not be easily monitored because they obtained their phone lines from Pakistan.[45] In 2005, citing deteriorating security conditions in Nepal due to Maoist violence, the Nepali king imposed authoritarian rule and a week-long media blackout and cut off all Internet access in the country.

In countries whose governments consider free access to information and unrestricted freedom of expression to be threats to social stability and public order, filtering is overwhelmingly targeted at local language content and country-specific issues.

China, Myanmar, and Vietnam filter a significant portion of content addressing their own human rights record and practices. Both China Netcom and China Telecom chose to block only one of the major international news organizations tested—the BBC—but they denied their users access to a significant number of overseas Chinese-language media representing different positions on the political spectrum. News in languages spoken by ethnic minorities in contested regions was also blocked in China. In Vietnam, sites only in English or French were rarely blocked, but sites in Vietnamese only tangentially or indirectly critical of the government—such as those with content focusing on local communities,

world news, or voicing strong anti-Communist sentiments—were inaccessible. In Pakistan, though Balochi and Sindhi independence and human rights sites have been filtered, other Web sites pertaining to Pashtun secessionism were fully accessible. In this case, filtering may be seen as unnecessary, as the majority of Pashtuns are illiterate in their local language.

Transparency

All countries in Asia engaged in technical filtering exhibited a lack of transparency in the legal authorization, technical processes, or implementation of filtering. Governments chose to remain silent on their source of authority to filter content from its citizens, or relied on indirect or implicit authority found in existing laws and regulations. Citizens in many countries were not put on notice of filtering as it occurred, and instead the cause of content inaccessibility was identified to be the result of inadvertent or unintentional error. Virtually all governments in Asia have yet to develop procedures for official notification of blocking to Web site owners, or appeal mechanisms for individuals to challenge blocking decisions in independent tribunals.

Governments often fail to disclose the extent of filtering to the general public. One notable exception is Singapore: before most Asian countries even had infrastructure in place to begin engaging in technical censorship of the Internet, Singapore announced in 1999 that a list of 100 pornographic Web sites would be blocked by the three major ISPs. As a "gesture of concern" to demonstrate the government's commitment to "Asian" values,[46] this figure has been continually cited in coverage of Internet censorship in Singapore, though the extent of actual filtering has remained symbolic.

In South Korea, state regulation (through the Internet Content Filtering Ordinance in 2001)[47] reportedly required ISPs to block as many as 120,000 Web sites on a state-compiled list, as well as mandating that Internet access facilities accessible to minors, such as public libraries and schools, install filtering software.[48] However, ONI testing indicated that Internet filtering in South Korea is not as extensive as reports have suggested. In Thailand as well, the distinct lack of transparency in the filtering process has persisted through the change in Thai governments. Adding to the uncertainty, a range of figures for the number of sites blocked by the Thai government continues to be circulated but not confirmed. A Thai police Web site citing the number of blocked sites at over 34,000 sites since 2002 has been taken down.

However, both South Korean and Thai ISPs do employ a blockpage, the most transparent notification of filtering. For example, sites blocked by KorNet through DNS tampering in South Korea resolve to a blockpage hosted by the police at 211.253.9.250. This blockpage not only states that the page has been lawfully blocked but also displays the user's IP address, which suggests the possibility of tracking the viewers that have visited the blocked site. Only a few countries provide clear notice that access is being denied because of proscribed content. In contrast, China's filtering methods are set up so that users in China who cannot access content due to IP address blocking, DNS tampering, or keyword search string filtering receive a network timeout or error page. When a keyword block is triggered, further requests made to the target site (IP address) are blocked (including attempts to access otherwise permissible sites) for a variable period ranging from five to thirty minutes.

Civil society mobilization

In Asia, civil society groups (as characterized/defined by Deibert and Rohozinski in Chapter 6) have carved out a prominent role in monitoring Internet censorship, advocating for greater access to information and freedom of expression and creating a space for issues shut out or marginalized in mainstream discourse. In response to the collateral blocking of the entire Blogspot

domain in India and Pakistan, bloggers and other loosely based coalitions mobilized quickly to generate media attention to the blocking and called for government transparency in the process.

Vigilant monitoring and advocacy by civil society activists in India, rather than government disclosure, has contributed to a greater understanding of technical filtering processes there. For example, the July 13, 2006, notice to block seventeen Web sites in the wake of the Mumbai train bombings issued by CERT-IN was not reproduced on any official government Web site but scanned and posted on an individual's blog. A number of individuals have filed requests seeking greater disclosure about the criteria and authorization for filtering under the 2005 Right to Information Act, but information has not been forthcoming.

Similarly, in Pakistan, the government never provided an official declaration confirming the blanket block on Blogspot.com since March 2006 or the rationale for it. Rather, the investigation and awareness-building around the controversial overblocking was initiated by two individuals through their "Don't Block The Blog" campaign. In the months after two Malaysians became the first bloggers to be sued for defamation in January 2007, bloggers in Malaysia and around the region formed the protest campaign "Bloggers United, No Fear," organized a legal defense fund trusteed by Datin Paduka Marina Mahathir, the daughter of former Prime Minister Mahathir Mohamad, and initiated a boycott of the plaintiff New Straits Times.

Many countries in Asia have achieved highly restricted media environments, and the Internet has become a tool for savvy civil society activists who must operate in them. Commonly the organization and resources required to shut down the Internet as an alternative medium of communication are far more expensive than the requirements of transmitting information online. For example, for many months in 2005 Radio Free Asia had been reporting about villagers in Shanwei in China's Guangdong province. These villagers had been protesting the construction of a wind power plant that would threaten their livelihoods and provide them with inadequate compensation for their expropriated land. After news about the police shooting and killing several Shanwei villagers broke in December 2005, the government attempted to suppress information about the incident by shutting down cybercafés in neighboring areas, cutting off Internet access to residents, stopping queries for the town's name on search engines, and erasing blogs mentioning the incident as soon as they were posted.[49] In spite of a lockdown in the area, a rights defense group was able to conduct an investigation into the incident and post it online.[50]

Conclusion

Notwithstanding a diverse range of approaches to Internet censorship, most of the governments in Asia where ONI conducted in-country testing are expanding their mandate to filter sensitive content, both technically and through "soft controls" such as legal regulation and delegated liability. Technical filtering is far from refined in most Asian countries, but is becoming an increasingly important tool in an armament of possible controls on free expression and the flow of information. It is also most clearly demarcated along national lines rather than using any regional or categorical formula. Accordingly many Asian governments focus overwhelmingly on content relating to sensitive political information and in local languages. Although filtering has been adopted as state policy for many Asian countries, the practices and implications of filtering continue to be contested.

Author: Stephanie Wang

NOTES

1. ICT Statistics, International Telecommunications Union, http://www.itu.int/ITU-D/ict/statistics/ict/index.html.
2. China Internet Network Information Center Report, Nineteenth Statistical Report on the Development of the Internet in China, (*di shijiu zhongguo hulian wangluo fazhan zhuangkuang tongji baogao*), issued January 23, 2007.
3. Ibid.
4. Paul Budde Communication Pty Ltd., India-Key Statistics and Telecommunications Market Overview, July 30, 2006, p. 2.
5. Paul Budde Communication Pty Ltd., Nepal: Telecoms Market Overview and Statistics, July 30, 2006, p. 11.
6. World Bank, World Development Indicators (2006), http://devdata.worldbank.org/external/CPProfile.asp?PTYPE=CP&CCODE=AFG; *Vision 2020: Islamic Republic of Afghanistan Millennium Development Goals Report 2005,* p. 123, p. 21
7. International Telecommunication Union, *World Telecommunication Indicators 2006.*
8. See Kristin Kalning, "Forget reality TV. In Korea, online gaming is it," MSNBC.com, February 21, 2007, http://www.msnbc.msn.com/id/17175353/.
9. Internet World Stats, Singapore, http://www.internetworldstats.com/asia.htm.
10. Terence Lee, "Internet control and auto-regulation in Singapore," Surveillance & Society 3(1): 74–95, http://www.surveillance-and-society.org/articles3(1)/singapore.pdf.
11. InfoComm Development Authority (IDA), Statistics on Telecom Services for 2006 (July–December), http://www.ida.gov.sg/Publications/20061205181639.aspx (listing 1,489,500 residential dialup subscriptions and 657,900 residential broadband subscriptions as of October 2006).
12. 2005 Information and Communication Technology Survey. National Statistical Office: Thailand, http://web.nso.go.th/eng/en/stat/ict/ict05_rep.pdf. See also Paul Budde Communication Pty Ltd., Thailand-Internet, 2006, p. 1.
13. Paul Budde Communication Pty Ltd., Telecommunication Sector Snapshot: Thailand, 2006.
14. China Internet Network Information Center Report, Nineteenth Statistical Report on the Development of the Internet in China, (*di shijiu zhongguo hulian wangluo fazhan zhuangkuang tongji baogao*),issued January 23, 2007.
15. Internet and Mobile Association of India, Internet in India:2006, http://www.iamai.in/research_index.php3.
16. 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;
17. Terence Lee, "Internet control and auto-regulation in Singapore," Surveillance & Society 3(1): 74–95, http://www.surveillance-and-society.org/articles3(1)/singapore.pdf.
18. See Vincent Lim, "Blogging for Democracy in Nepal," AsiaMedia, April 13, 2006, http://www.asiamedia.ucla.edu/article.asp?parentid=43000.
19. See Mark Glaser, "Nepalese Bloggers, Journalists Defy Media Clampdown by King," Online Journalism Review, February 23, 2005, http://www.ojr.org/ojr/stories/050223glaser/.
20. http://advertising.microsoft.com/asia/NewsAndEvents/PressRelease.aspx?Adv_PressReleaseID=296.
21. See http://ohmynews.com; Jun Kwanwoo, "'Citizen journalism' wins hearts and minds," Dawn, March 30, 2007, http://www.asiamedia.ucla.edu/article.asp?parentid=66921.
22. See Christopher M. Schroeder, "Is this the Future of Journalism?" Newsweek, June 18, 2004, http://www.msnbc.msn.com/id/5240584/site/newsweek/.
23. Paul Budde Communication Pty Ltd., 2006, Vietnam:Internet, p. 10, July 30, 2006. See also John Boudreau, "Bay Area Entrepreneur Leads Way in Online Gaming in Vietnam," The Mercury News, January 17, 2007, http://www.mercurynews.com/mld/mercurynews/business/16475618.htm.
24. China Internet Network Information Center Report, Nineteenth Statistical Report on the Development of the Internet in China, (*di shijiu zhongguo hulian wangluo fazhan zhuangkuang tongji baogao*),issued January 23, 2007.
25. Xinhua News Agency, "China has 20.8 million bloggers," January 10, 2007.
26. National Electronics and Computer Technology Center (NECTEC), Thailand MICT Indicators 2005 (February 2005), http://iir.ngi.nectec.or.th/download/indicator2005.pdf.
27. The Press Trust of India, "Indians prefer good-old diary to blogs," November 27, 2006.
28. Deutsche Presse-Agentur, "Vietnam youths arrested over internet chats released after 9 months," August 16, 2006. See also Human Rights in China, Press Release, "Dissident writer Zhang Lin to be tried next week," June 15, 2005, http://www.hrichina.org/public/contents/press?revision_id=22932&item_id=22931.
29. Xinhua News Agency, "China to issue new regulations to censor online video programs," August 16, 2006.

30. See Article 19, Freedom of Expression and the Media in Thailand, December 2005, at 38. The 1997 Constitution has since been abrogated. Council for Democratic Reform, Announcement no. 3, September 17, 2006.
31. See Freedom Against Censorship Thailand Web site, http://facthai.wordpress.com, (accessed April 4, 2007).
32. U.S. Department of State, Country Reports on Human Rights Practices 2006: Singapore, at 1.e., 2.a., 2.d., 3, http://www.state.gov/g/drl/rls/hrrpt/2006/78790.htm.
33. Bangkok Post, "Defamation law being misused, seminar told," January 10, 2005, http://www.asiamedia.ucla.edu/article.asp?parentid=19333.
34. South China Morning Post, "Newspaper sues Internet bloggers for defamation," January 19, 2007, reprinted at http://www.asiamedia.ucla.edu/article.asp?parentid=61629.
35. In August 2003, CERT-IN issued an order to ISPs to block the mailing list kynhun on Yahoo! Groups belonging to the militant outfit Hynniewtrep National Liberation Council. See http://pib.nic.in/archieve/lreleng/lyr2003/rsep2003/22092003/r2209200314.html.
36. See Korea Internet Safety Commission, http://www.icec.or.kr/.
37. The Irrawaddy Online, "Something is better than nothing," April 2, 2004, http://www.irrawaddy.org/art/2004/april01.html.
38. See Shivam Vij, "The discreet charms of the nanny state," National Highway, October 2006, http://www.shivamvij.com/2006/10/the-discreet-charms-of-the-nanny-state.html.
39. Reporters Without Borders, "Internet increasingly resembles an Intranet as foreign services blocked," July 4, 2006, http://www.rsf.org/article.php3?id_article=18202; *The Irrawaddy,* "Junta blocks Google and Gmail," June 30, 2006, http://www.irrawaddy.org/aviewer.asp?a=5924.
40. See Cherian George, "One country, two systems; for how long?" http://singaporemedia.blogspot.com/2007/03/one-country-two-systems-for-how-long.html
41. U.S. Department of State, Country Reports on Human Rights Practices 2006: Singapore, at 2.a., http://www.state.gov/g/drl/rls/hrrpt/2006/78790.htm.
42. See Malaysia Multimedia Super Corridor Web site, http://www.msc.com.my/msc/rollout_status.asp.
43. See, for example, Star Online, "Government looking at gaps in Printing Act," July 27, 2006, http://www.thestar.com.my/news/story.asp?file=/2006/7/27/nation/14961817&sec=nation ("The Government will study if the Printing Presses and Publications Act should be amended to include the electronic media and the Internet media.")
44. Malaysian Communications Multimedia Act of 1998, § 211(1). See Reme Ahmad, "Case revives debate of freedom of speech versus the right to redress," *The Straits Times,* January 20, 2007.
45. BBC News, "Taleban outlaw Internet," July 13, 2001, http://news.bbc.co.uk/2/hi/south_asia/1437852.stm.
46. Terence Lee, "Internet control and auto-regulation in Singapore," Surveillance & Society 3(1): 74–95. http://www.surveillance-and-society.org/articles3(1)/singapore.pdf.
47. Electronic Frontiers Australia, Internet Censorship: Law & Policy Around the World (2002), http://www.efa.org.au/Issues/Censor/cens3.html#sk.
48. See, for example, Han Chae-yun and Yi Huso, "On-again and off-again: Korean on/off-line LGBTQ/lban community blocked," The Sungkyun Times, September 2002, http://web.skku.edu/~sktimes/251/society.html.
49. Esther Pan, "China's angry peasants," Foreign Council on Foreign Relations, http://www.cfr.org/publication/9425/#4; International Freedom of Expression eXchange, "Beijing imposes new blackout on village shootings," http://www.ifex.org/alerts/layout/set/print/content/view/full/71219/.
50. See EastSouthWestNorth blog, at http://www.zonaeuropa.com/20060112_1.htm.

For information about special quantity discounts, please e-mail special_sales@mitpress.mit.edu.

This book was set in Swis721 on 3B2 by Asco Typesetters, Hong Kong.
Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access denied : the practice and policy of global Internet filtering / edited by Ronald Deibert . . . [et al.].
p. cm. — (The information revolution & global politics series)
Includes bibliographical references and index.
ISBN 978-0-262-54196-1 (pbk. : alk. paper) — ISBN 978-0-262-04245-1 (hardcover : alk. paper)
1. Computers—Access control. 2. Internet—Censorship. 3. Internet—Government policy. I. Deibert, Ronald.
QA76.9.A25.A275 2008
005.8—dc22 2007010334

10 9 8 7 6 5 4 3 2 1