Thailand

Amid political crisis, a deep social divide, and the uncertainty of royal succession, Thailand's Internet has become a contested terrain of various political views and movements. While the government has employed both legal and technological means to censor, filter, and control Internet content and communication, service providers and users resort to intermediary censorship and self-censorship, and dissidents resist the control, using evasion and circumvention tools and campaigning for freedom and transparency. Lèse-majesté, a deep-seated tradition in Thai society, has become a tool for clamping down on dissenting opinion and a basis for many online users to integrate state control into their own cyber behavior as they participate voluntarily in the surveillance and censorship of the Internet.

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)	7,258
Life expectancy at birth, total (years)	63
Literacy rate, adult total (percent of people age 15+)	64.9
Human Development Index (out of 169)	92
Rule of Law (out of 5)	1.6
Voice and Accountability (out of 5)	1.5
Democracy Index (out of 167)	57 (Flawed democracy)
Digital Opportunity Index (out of 181)	151
Internet penetration rate (percentage of population)	25.8

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. See Introduction to the Country Profiles, pp. 222–223.

Background

Thai politics, long famous for coups and military dominance, shifted course in 2001 with the emergence of a single-party civilian government led by Prime Minister Thaksin Shinawatra and his Thai Rak Thai (TRT) Party. The TRT Party won landslide victories in two general elections in 2001 and 2005, becoming the second party in 73 years to form a single-party government. Thaksin, a former telecommunications tycoon who made his fortune from monopoly government concessions, was also the first prime minister to have completed a full four-year term in office. Despite his popularity, Thaksin is widely criticized for his authoritarian traits, outspokenness, and conflict of interest over his family business—Shin Corporation. A deal to sell a major stake in Shin Corporation to an investment firm owned by the Singaporean government mobilized a large number of the urban middle class to rally for Thaksin's resignation,[1] culminating in the formation of a royalist anti-Thaksin movement called the People's Alliance for Democracy (PAD), or the "yellow shirts." This public anger and protest was a prelude to the military coup that toppled Thaksin on September 19, 2006.[2]

Years of political turmoil followed the coup, and Thailand's political situation remains volatile. The rift between the United Front for Democracy against Dictatorship (UDD), or the "red shirts," which supports the ousted Thaksin, and the Yellow Shirts has deepened into a social divide. The opposing forces have become a reflection of the clash between an urban middle class on one side and the rural poor on the other.[3] Demands by the UDD for fresh elections resulted in a series of protests in Bangkok,

with most of the protestors coming from outside the city. During April and May 2010, the demonstrations erupted into violence when military crackdowns were launched in order to disperse the antigovernment protestors.[4] Up to 90 people were killed and almost 2,000 were injured in the political mayhem that gripped the country between March 12 and May 19, 2010.[5] During the political unrest, the government issued a State of Emergency Decree on April 8, 2010, to block 36 Web sites that primarily had content sympathetic to the red shirts.[6] In addition to this state-sanctioned censorship, the Internet community in Thailand also appears to censor itself.

Internet in Thailand

The number of Internet users in Thailand has increased exponentially from 2.3 million in 2000 to 18.3 million in 2009,[7] resulting in an estimated penetration rate of 25.8 percent in 2009.[8] In 2010 international bandwidth for the entire country was 156,680 Mbps, while domestic bandwidth was 721,217 Mbps.[9] Nearly half of all Internet users are between 20 and 29 years old. Nearly half, 46.8 percent, of users access the Internet in educational institutions, 33.4 percent at home, and 29 percent at work.[10] Fifty-five percent of Internet users are concentrated in Bangkok and the greater Bangkok area.[11] Of these users, 43.5 percent access the Internet through broadband.[12]

According to the data from the National Electronics and Computer Technology Center (NECTEC), Thailand has six international Internet gateways (IIGs), which also serve as national Internet exchanges.[13] There are about 20 Internet service providers (ISPs) that are active and carrying Internet traffic. In 2010, TOTNET, TRUE, and 3BB dominated the market, holding market shares of 40.24 percent, 29.79 percent, and 25.60, respectively.[14] Half the operating ISPs are semiconcessionaires with 35 percent of their shares held by default by CAT Telecom,[15] a corporatized state enterprise and a long-standing international carrier monopoly.[16] The remaining ISPs are new operators that emerged as a result of the telecommunications reform following the establishment in 2004 of the National Telecommunications Commission (NTC), the country's first independent regulator of telecommunications. The commission has been issuing licenses for telecommunications services and Internet services since 2005. So far, a total of 130 licenses have been issued for telecommunications services, and 132 for Internet.[17] These figures reflect a two-tiered structure of Internet regulation. On one side, there are the prereform semiconcessionaires that are highly liable to CAT Telecom, which answers directly to the Ministry of Information and Communications Technology (MICT). On the other side, there are the postreform ISPs that operate under licenses issued from the NTC. This structure leads to somewhat of a double standard in Internet regulation and filtering.

The government has established the Government Information Network (GIN) to promote the level of information communication technology (ICT) employed in its

agencies ranging from ministry level to department level. The main objective of this network is to create an e-government, which will pave the way for a government Internet gateway solely for state agencies.[18]

The top three most popular Web sites are sanook.com, kapook.com, and mthai.com, all of which are Web portals.[19] Thai users' primary purposes for accessing the Internet are to seek news and information (29.7 percent), to send e-mails (21.9 percent), and to engage in e-learning (8 percent).[20] The number of users accessing social networking Web sites has steadily increased. Within a span of nine months in 2010, the number of Facebook users in Thailand more than doubled from 2 million in January to more than 5 million in September.[21] The sharp increase in use and growth of awareness about Facebook can be attributed to the political crisis in March to May 2010. The extensive media censorship enforced under emergency decree triggered political discourse to move to the highly interactive and participatory platform. Given Facebook's recent announcement of 500 million active users worldwide,[22] this means that Thailand now accounts for more than 1 percent of the total active Facebook population worldwide.

Legal and Regulatory Frameworks

The MICT is responsible for ICT policy and oversight across the country. The second ICT master plan (2009–2013) aims to provide countrywide broadband, the so-called National Broadband Policy.[23] This is a part of the ICT Scheme 2020, which was drafted as a framework to develop the national ICT infrastructure. One of the main objectives of the master plan is to increase broadband Internet access to 80 percent of the population by 2015.[24]

The NTC is the country's telecommunications regulatory authority. Apart from its main responsibility in managing radio and telecommunication frequencies, the NTC also has the authority to grant licenses for Internet service, international Internet gateways, and Voice over Internet Protocol (VoIP) service.

An Internet filtering regime began in Thailand in 2002 with the establishment of a filtering unit within the MICT called the Cyber Inspector. The Cyber Inspector focused its filtering activity on issues such as pornography, negative comments about the monarchy, gambling, terrorism, and separatist movements.[25] However, its existence and role were widely questioned by the public because of a lack of legal grounds for filtering. The legalization of Internet filtering began in 2007 with the enactment of the controversial Computer Crime Act. This law was the first to be passed during the interim legislature appointed by the military junta. Apart from carrying broad-based provisions on content regulation, a tradition quite unusual for cybercrime law, this relatively new law also allows competent officials (who are appointed by the minister of ICT) to apply for court orders to seize computer equipment and to block

Web sites.[26] Furthermore, since 2008, an automatic URL filtering system has been installed at IIGs under CAT Telecom to filter objectionable materials, with lèse-majesté content being the prime target.[27]

Lèse-majesté, which refers to punishment for any negative public remarks about the monarchy, is strongly enforced in Thailand. The Thai criminal code specifies that whoever "defames, insults or threatens the King, Queen, the heir-apparent or the Regent" can be jailed for three to 15 years.[28] Although lèse-majesté was not included as a deterrent to Internet content in the law, it was incorporated under the broad provision of national security because the Thai nation-state is understood to rest on three pillars—the nation, the Buddhist religion, and the monarchy.[29] For this reason and because of the social divide between supporters of the monarchy and supporters of Thaksin Shinawatra, lèse-majesté has been increasingly invoked to censor Web sites. According to recent research, there was one court order to block two URLs in 2007, whereas in 2008 there were 13 court orders to block 2,071 URLs.[30] There were 64 orders in 2009 resulting in 28,705 Web sites ordered blocked. The number of Web sites ordered to be blocked rose to 43,908 in 2010.[31] Within three years after the enforcement of the Computer Crime Act, there have been 117 court orders to block access to 74,686 URLs.[32] Given the far-reaching power of this act, there is increasing evidence that this law is being employed as a political tool.[33]

A recent notable case of lèse-majesté being used to prosecute individuals for online actions is that of Chiranuch Premchaiporn, Web master of the popular online news portal Prachatai. Chiranuch was first charged in March 2009 under Section 15 of the Computer-Related Offenses act for intermediary liability or consent/negligence of operators for offenses to be committed. These charges were brought down because of alleged lèse-majesté comments posted on the Prachatai forum by users, which Chiranuch claims were removed immediately following the first notice from police. In September 2010, she was arrested and served new charges following reentry into Thailand after attending a Google-sponsored conference on Internet liberty. These further charges included lèse-majesté offenses for publishing an interview on Prachatai with a Thai man who was arrested and charged with lèse-majesté for refusing to stand during the royal anthem in a cinema.[34] A trial started in February 2011, with a verdict expected in April 2011. Chiranuch faces ten separate charges, each of which carries a maximum sentence of five years in jail. This case is a stark example of Thai legislation used to prosecute individuals for intermediary liability for lèse-majesté content and has raised concerns for freedom of expression in communities across the world.[35]

To bypass Internet censorship, many activists and dissidents use anonymizers and circumvention software.[36] With the recent enforcement of the State of Emergency Decree, online users and online service providers (OSPs) also self-censor or strictly monitor content to avoid prosecution under the Computer Crime Act. Public

education and campaigns against the government's Internet control have also been carried out, mostly by the so-called Thai Netizen Network (TNN), a relatively new local nongovernmental organization (NGO) that advocates for Internet freedom. Increasingly, TNN has become allied with several international NGOs concerned with media freedom, including Freedom House and the Electronic Frontier Foundation.

Surveillance

Without an explicit privacy law in place, several data surveillance schemes have been administered since at least 1981 in Thailand without adequate legal safeguards, including the computerized and online civil registration system, a microchip national ID card system, a computerized criminal records database system, and surveillance cameras in public areas.[37] However, the public generally views these systems as part of the long-standing civil registration system and data infrastructure and not as surveillance schemes. For online surveillance, state-controlled IIGs and ISPs have been instructed to look into interactive communication in online forums hosted under their networks, focusing on lèse-majesté speech, and to give a 30-minute time frame for taking down such content. While the new surveillance scheme is not public knowledge, members of the public are unlikely to object to it, since filtering is rationalized on the grounds of lèse-majesté. More technologically savvy dissidents and civic workers have evaded the surveillance by relocating to host services overseas and by using circumvention software.

In a recent example of cybercrime law enforcement, local Internet advocates and media for the first time posited privacy rights as being undermined by law enforcers' zeal to track and crack down on sources of rumors surrounding the king's ailing condition.[38] This development followed the arrest of two suspects who posted the "problematic information (about the king)" in two popular online forums.[39] Prompted by this incident, the Department of Special Investigation (DSI) reportedly sought court orders to look into the e-mail communication of all the people who had posted on related topics on the two forums.[40]

Many Internet users also participate in online surveillance of lèse-majesté. For instance, a fan page called Social Sanction was developed for reporting lèse-majesté comments posted on Facebook.[41] A teenage girl was socially reprimanded after her damaging posts on the king were publicized on the Social Sanction page. Her admission to a prestigious university was denied on grounds of social misconduct, stemming from her "problematic" online speech.[42]

Although there is no comprehensive national law that addresses privacy in Thailand, there is a constitutional guarantee for the right to privacy in the section on protection of rights and liberties of citizens in the current constitution of 2007. Existing laws contain no direct stipulations about violation of "privacy" per se.[43] There is

a section in the Freedom of Official Information Law (passed in 1997) that addresses protection of personal data kept in government files.[44]

A draft data protection law has been in existence since 1996 but has yet to materialize. In the latest development, in October 2009, the Cabinet agreed in principle to forward the draft law for Parliament reading.[45] The next step will be to appoint commissioners for the reading of the draft law. However, with other legislative priorities and inherent political instability, the draft law was sidestepped and has not yet made it to the legislative agenda.

Meanwhile, the new Cybercrime Law passed in 2007 has delegated full authority to state officials in surveillance, censorship, and control of Internet information and communication. For instance, Section 18 of this law authorized designated competent officials to do the following:

- Summon an alleged party to appear, report to, or send documents, information, or evidence.
- Request computer-based traffic information and other information that concerns Internet users from service providers and parties involved.
- Duplicate computer information and computer-based traffic information.
- Decrypt, censor, and access computer systems, computer information, computer-based traffic information, or equipment used to store computer information.
- Confiscate or "freeze" any computer system.[46]

The 2007 Computer Crime Act required all service providers—ISPs, OSPs, Web masters, Web moderators, and Internet cafés—to keep a log file of their users including IP addresses for 90 days.[47] This requirement necessitated setting up an identification and authentication clearance system for users as a condition for accessing the Internet—in other words, a surveillance system operated by service providers.

Findings from a series of focus groups on surveillance and privacy conducted in Bangkok found that there is a disparity with regard to public perception and knowledge of information privacy between different socioeconomic classes.[48] Those from the upper socioeconomic strata are generally more concerned with privacy rights and threats from personal data collection and use, and possess a greater understanding of information privacy, while those from a lower socioeconomic background tend to be less concerned with surveillance practices because they do not see privacy as being a part of their basic needs; rather, they are more concerned with making ends meet. The latter were also found to be less likely to challenge surveillance practices because they have less knowledge of surveillance technologies and a feeling of general powerlessness vis-à-vis the state.[49]

In recent years, new Internet applications such as social networking Web sites have emerged as popular communication tools among the younger generations in Thailand. Parallel to the emergence of such applications is the rise of new privacy

challenges—for instance, the unintended consequences of posting sensitive personal information and confusion over privacy settings. While Thailand ranks in the top 20 fastest-growing user countries for Facebook, little awareness has been raised about the privacy implications of these popular applications.

There is a dearth of advocacy work in Thai civil society when it comes to privacy. Local NGOs working in the areas of information and communication are mainly focused on freedom of expression, freedom of information, consumer protection, intellectual property, and access rights. However, there is no identifiable civic entity whose main focus is privacy. The last time a privacy issue emerged at a public level, it was advocated by a consumer-protection NGO that viewed the mass texting of greeting messages from the then-incoming Prime Minister Abhisit Vejjajiva to all mobile phone users as a violation of privacy.[50]

ONI Testing Results

OpenNet Initiative conducted testing between April and May 2010 following Thailand's State of Emergency Decree invoked on April 8, 2010. Testing was conducted on two major Thai ISPs: TRUE and TOTNET. Results indicate that these ISPs primarily block content related to political opposition sites, pornography, gambling, and circumvention tools. A central focus of this blocking is on political content related to the red shirts and Thai-language content.

Testing by ONI on the 36 Web sites ordered blocked determined that neither TRUE nor TOTNET filtered the entirety of the Thai government's block list. TOTNET blocked only ten URLs from the list, and TOTNET filtered this same set and an additional 13 for a total of 23 URLs. The sites found blocked included pro–red shirt Web sites (http://thaipeoplevoice.org, http://sunshine.redthai.org, and http://xat.com/uddtoday) and news sites that provided updates on the unrest (http://prachatai.com and http://thaipeoplevoice.org). Pages on social media Web sites used by the red shirts to disseminate messages and organize demonstrations were also blocked on both ISPs, including the presence of the United Front for Democracy and Dictatorship on Twitter (http://twitter.com/uddtoday), Facebook (http://facebook.com/note.php?note_id=344691628328), and Ning (http://uddtoday.ning.com). Web sites belonging to the anticoup site (http://19sep.com) and the Patani United Liberation Organization (http://puloinfo.net) that were blocked in 2007 were found accessible in 2010 testing.

Technical analysis of the data from TRUE and TOTNET found that filtering was implemented similarly by both ISPs. Consistent with past ONI findings, when users on TRUE and TOTNET attempt to access blocked content they are redirected to an MICT block page. TRUE's block page notified users that the content was blocked by order of the emergency decree, whereas TOTNET's block page did not.

While both ISPs similarly implemented filtering, ONI found that filtering was inconsistent between them, and that the overall level of filtering on TOTNET was greater than that of TRUE in all categories where filtering was found. For instance, TOTNET blocked circumvention tools and anonymous proxy sites (e.g., http://proxify.com, http://anonymouse.com) and the online gambling Web site http://gamebookers.net, whereas TRUE did not. Testing results also show that the blocking of pornography remains inconsistent and observed a slight increase in the number of English-language pornography sites blocked. No Thai-related pornography sites were found blocked. The site http://sex.com was the only pornographic content from 2007 that continues to be blocked.

These overall results are consistent with findings from 2007 testing and show that filtering continues to be inconsistently practiced in Thailand and that government block lists are not uniformly implemented across ISPs.

Conclusion

As a result of highly volatile conditions and the politicization of online communication, Internet control in Thailand in the post-2006-coup period features a combination of approaches—technical, legal, and social. Conventional ISP-level filtering, based on state-mandated block lists, has been complemented by automatic URL filtering at the IIG level as well as filtering at other points in the network, particularly at the OSP level. Due to the enforcement of the new cybercrime law, which imposes severe intermediary liability, OSPs have emerged as important chokers for censorship, since they host social networking services, blogs, and online political forums—all of which constitute the much-needed public sphere in the climate of otherwise suppressed speech. Apart from filtering out problematic content and denying hosting space to politically risky content providers, OSPs also construct an identification clearance system to enable surveillance of users and potential rule breakers.

In addition to the new Cybercrime Law, which legalizes Internet blocking through court orders and helps enforce other filtering mechanisms, two other laws contribute directly to the new regime of Internet control: the State of Emergency Decree and lèse-majesté laws. While the former made censorship seem inevitable in the face of crisis, the latter, as an entrenched social norm, helped justify it. What is more alarming is how members of online communities engaged in cyber witch-hunting using lèse-majesté as a powerful rationale to publicly condemn and reprimand those who represent dissenting opinions.

Such controlling schemes have not only created a chilling effect in cyberspace as users and service providers resort to self-censorship and intermediary censorship, but have also given rise to struggles and resistance. More technologically capable

dissidents have evaded the control using anonymizers and circumvention tools, while civic organizations advocating for online freedom of expression have introduced public education and regularly campaign against government Internet control, allied with international NGOs advocating on similar issues.

Notes

1. Shino Yuasa, "Anti-Thaksin Groups Launch Boycott over Temasek-Shin Corp Deal," Manager Online, March 9, 2006, http://manager.co.th/Home/ViewNews.aspx?NewsID=9490000033125.

2. Pasuk Phongpaichit and Chris Baker, "Thaksin's Populism," *Journal of Contemporary Asia* 38, no. 1 (2008): 62–83.

3. Economist Intelligence Unit Limited, *Country Report: Thailand*, Economist Intelligence Unit Limited, 2010.

4. "Army's Power at Peak since Crackdown," *Bangkok Post*, June 19, 2010, http://www.bangkokpost.com/news/local/39016/army-power-at-peak-since-crackdown.

5. Ibid.

6. Anuchit Nguyen, "Thai Government Blocks Protest Web Site after Emergency Decree," *Bloomberg Business Week*, April 7, 2010, http://www.businessweek.com/news/2010-04-07/thai-government-blocks-protest-web-site-after-emergency-decree.html.

7. National Electronics and Computer Technology Center, "Internet User in Thailand," November 15, 2010, http://internet.nectec.or.th/webstats/internetuser.iir?Sec=internetuser.

8. 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.

9. National Electronics and Computer Technology Center, "Thailand Internet Bandwidth," August 18, 2010, http://internet.nectec.or.th/webstats/bandwidth.iir?Sec=bandwidth.

10. Office of National Statistics, *ICT Household 2009*, Bangkok: Thana Press, 2010.

11. National Electronics and Computer Technology Center, *Internet Users Profile of Thailand 2552 (2009),* http://pld.nectec.or.th/websrii/images/stories/documents/books/internetuser_2009.pdf.

12. Office of National Statistics, *ICT Household 2009*.

13. The six IIGs are CAT Telecom Plc, TOT Plc, TRUE Corporation, Thai Telephone and Telecommunications (TT&T), ADC, and CS Loxinfo. Of these six IIGs, CAT Telecom Plc and TOT Plc were former state enterprises and monopoly telecommunication companies, while TRUE and TT&T are long-time telecommunications concessionaires. Only ADC and CS Loxinfo are new market entrants after the telecommunications reform in 2005. For more discussion, see Thaweesak Koanantakool, "Important Internet Statistics of Thailand," August 24, 2007, Internet Information

Research Network Technology Lab, http://internet.nectec.or.th/document/pdf/20070824_Important_Intenet_Statistics_of_Thailand.pdf.

14. National Telecommunication Commission of Thailand, *Telecommunication Market Report 2010,* Bangkok: NTC, 2010.

15. Pirongrong Ramasoota, "Internet and Democracy in Thailand," in *Rhetoric and Reality: The Internet Challenge for Democracy in Asia*, ed. Indrajit Banerjee (Singapore: Eastern Universities Press: 2003), 297.

16. Although CAT Telecom's shares are controlled by the Ministry of Finance, the entity is under the bureaucratic structure of the Ministry of Information and Communication Technology.

17. National Telecommunications Commission, Unpublished Data Submitted to the Commission in the reading of the Frequency Allocation Organization and Regulation of Broadcasting and Telecommunications draft law, 2010.

18. Ministry of Information, Communication and Technology, "Government Information Network: GIN," http://203.113.25.35/gin/rationale.htm.

19. Internet Innovation Research Center, "Web Rank by Country: Thailand," http://truehits.net/index_ranking.php.

20. National Electronics and Computer Technology Center, *Internet Users Profile of Thailand 2552 (2009).*

21. Jon Russell, "Analysis: Thailand Passes Five Million Facebook Users," Asian Correspondent, September 7, 2010, http://www.asiancorrespondent.com/39989/analysis-thailand-passes-5-million-facebook-users.

22. Figures obtained from Facebook press release available at http://www.facebook.com/press/info.php?statistics, accessed February 7, 2011.

23. Ministry of Information, Communication, and Technology, "Broadband Policy," November 18, 2010, http://www.mict.go.th/article_attach/policy_Broadband.pdf.

24. Ibid.

25. See Pirongrong Ramasoota and Nithima Kananithinan, *Internet Content Regulation in Thailand*, 2003 Research report under the Media Reform Research Project. Supported by the Thailand Research Fund (TRF), http://www.tdri.or.th/reports/unpublished/media/number10.pdf.

26. Section 18, Thailand Computer-Related Offenses Act B.E. 2550, http://www.lib.su.ac.th/ComputerLaw50.pdf.

27. The existence of this automatic URL filtering system is not common public knowledge. Its existence was discovered by OpenNet Asia research, which revealed that a group of computer science researchers from Kasetsart University in Bangkok were commissioned by CAT Telecom, a state enterprise that runs major IIGs, to design the filtering system. For further details see

Pirongrong Ramasoota, "Internet Politics in Thailand after the 2006 Coup: Regulation by Code and a Contested Ideological Terrain," chapter 5 in this volume.

28. Thai Criminal Code B.E. 2499 (1956), Article 112. Unofficial English translation is available at http://www.samuiforsale.com/Law-Texts/thailand-penal-code.html.

29. Somboon Suksamran, *Buddhism and Politics in Thailand*. Singapore: Institute of Southeast Asian Studies, 1982.

30. Siriphon Kusonsinwut, Sawatree Suksri, and Oraphin Yingyongpathana, "Situational Report on Control and Censorship of Online Media, through the Use of Laws and the Imposition of Thai State Policies," *iLaw*, http://ilaw.or.th/node/632.

31. Ibid.

32. Ibid.

33. Peter Leyland, "The Struggle for Freedom of Expression in Thailand: Media Moguls, the King, Citizen Politics and the Law," *Journal of Media Law* 2, no. 1 (2010): 115–137.

34. "Thailand: Moviegoer Faces Prison for Sitting during Anthem," *New York Times*, April 24, 2008, http://query.nytimes.com/gst/fullpage.html?res=9506E1DF1E31F937A15757C0A96E9C8B63&fta=y.

35. For further details on lèse-majesté in Thailand, see Pirongrong Ramasoota, "Internet Politics in Thailand after the 2006 Coup: Regulation by Code and a Contested Ideological Terrain," chapter 5 in this volume; see also Shawn W. Crispin, "Internet Freedom on Trial in Thailand," Committee to Protect Journalists, February 5, 2011, http://www.cpj.org/blog/2011/02/internet-freedom-on-trial-in-thailand.php; Simon Montlake, "Web Site Editor's Trail in Thailand a Test Case for Media Freedom," *Christian Science Monitor,* February 4, 2011, http://www.csmonitor.com/World/Asia-Pacific/2011/0204/Website-editor-s-trial-in-Thailand-a-test-case-for-media-freedom.

36. For instance, Freedom against Censorship Thailand (FACT), an NGO that advocates on freedom of expression online, has offered free downloads of circumvention software on their Web site. See http://facthai.wordpress.com/links/softwares/.

37. Pirongrong Ramasoota, "State Surveillance, Privacy and Social Control in Thailand (1358–1997)," 2000, PhD dissertation, Simon Fraser University, Canada.

38. "Data-Interception Technology Sparks Privacy vs Safety Arguments," *Bangkok Post*, January 21, 2010, http://www.bangkokpost.com/print/31829.

39. Richard Frost, "Thai Stocks, Baht Slump on King's Health Speculation," Bloomberg, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aWSLmdQccvyo.

40. In this incident, two stock brokers were arrested and charged with spreading online rumors on two online forums, http://prathathaiwebboard.co.th and http://sameskywebboard.co.th, about the king's deteriorating health. Their postings led to the panic selling in the local stock market in November 2009. The Computer Crime Act allows action against computer users spreading information deemed detrimental to national security or false information that could cause

panic among the public. See James Hookway, "Thai Police Arrest Two Accused of Violating Internet Laws," *Wall Street Journal*, November 3, 2009, http://online.wsj.com/article/SB125712550983721881.html.

41. Poowin Buyavejchewin, "Internet Politics: Internet as a Political Tour in Thailand," *Canadian Social Science* 6, no. 3 (2010); "Political Battles Go Online," *Bangkok Post,* January 8, 2010, http://m.bangkokpost.com/articledetail.php?channelID=1&articleID=188908.

42. "Political Battles Go Online," *Bangkok Post*.

43. Privacy abuses in Thailand have typically been framed in terms of trespass, defamation, or breach of trust or confidence. For analysis of privacy-related laws in Thailand, see Ramasoota, "State Surveillance, Privacy and Social Control in Thailand (1358–1997)."

44. Chapter 3: Personal Information, Official Information Act B.E. 2540, http://www.oic.go.th/content_eng/act.htm.

45. "Cabinet to Consider Data Protection Law" [in Thai], Chaopraya News, October 14, 2010, http://www.chaoprayanews.com/2010/10/14/.

46. Section 18, Thailand Computer-Related Offenses Act B.E. 2550, http://www.lib.su.ac.th/ComputerLaw50.pdf.

47. Section 26, Computer Crime Act B.E. 2550 (2007), issued June 10, 2007, effective July 18, 2007. Unofficial English translation is available at http://www.prachatai.com/english/node/117.

48. See Pirongrong Ramasoota Rananand, "Information Privacy in a Surveillance State: A Perspective from Thailand," in *Information Technology Ethics: Cultural Perspectives*, ed. Soraj Hongladarom and Charles Ess (Hershey, PA: Idea Group Reference, 2007).

49. Ibid.

50. Tulsathit Taptim, "Did Abhisit Text Himself into More Trouble?" *The Nation*, July 16, 2010, http://www.nationmultimedia.com/home/2010/07/16/politics/Did-Abhisit-text-himself-into-more-trouble-30133903.html.

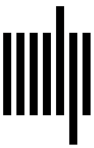
Access Contested

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