5 Internet Politics in Thailand after the 2006 Coup

Regulation by Code and a Contested Ideological Terrain

Pirongrong Ramasoota

In 2009, Thailand joined the rank of "a new enemy of the Internet," according to Reporters Without Borders.[1] This status is ironic, given the fact that the country's name means "land of the free" in Thai. This development marked a significant regress from a decade earlier when there was no cyber law and no regulator, only open Internet architecture and freedom as the central norm among first-generation Thai Internet users. Despite economic doldrums that followed a financial meltdown in 1997, freedom of expression and freedom of information in Thailand were markedly stable in the late 1990s.[2] The Thai Internet regulatory landscape gradually shifted, however, first with the establishment of the Ministry of Information and Communication Technology (MICT)[3] in 2002, which introduced the first Internet filtering policy, and later with the passing of the computer crime law in 2007, following the September 2006 military coup that overthrew the country's longest-ruling civilian administration in modern Thai history.

The period following the 2006 coup saw Thai politics bitterly divided between two opposing camps: red-shirted supporters[4] of the self-exiled former prime minister, Thaksin Shinawatra, who was ousted from power on charges of corruption and for disloyalty to the crown; and those who back the country's "network monarchy"[5]—a loose alliance of the palace, the military, the ruling Democrat Party, and the People's Alliance for Democracy (PAD), or the "yellow shirts."[6] This contest has also exhibited itself in the online sphere as powerful members of the network monarchy exercised control over Internet communication to maintain political stability while red-shirt dissidents and their supporters evaded and resisted the control through circumvention and online civic mobilization. Notably, the new computer crime law has been a potent force in constraining the behavior of Internet users as well as service providers through the new regulatory framework it imposes. In the postcoup years, the lèse-majesté offense—insulting the monarchy—has also been increasingly used to charge anyone writing or posting material deemed to be defamatory of Thailand's King Bhumibol Adulyadej or the royal family, and in blocking Internet content or shutting down Web sites.

In *Codes and Other Laws of Cyberspace*, Lawrence Lessig notes that four major regulatory elements are at play in Internet regulation—social norms, markets, technology (what he calls architecture), and law. Each of these elements, he argues, can directly limit individuals' actions in cyberspace through the different type of constraint each imposes, or they may work in combinations to constitute the "code" that regulates Internet users' behavior, that is, "regulation by code."[7] Norms constrain through the stigma that a community imposes; markets constrain through the price they exact; architecture constrains through the physical burdens it imposes; and law constrains through the punishment it threatens. Lessig emphasizes that architecture is the most sensible and influential modality of regulation. Nevertheless, he also notes that law can also change the regulation of architecture, especially when architecture (how the network is built and designed) is changed in order to realize a particular social end.

To extend Lessig's notion of regulation by code a bit further, a classical Marxist theory of ruling ideology is relevant if one considers the Internet beyond its role as conduit technology and thinks more deeply about its content and communication dimensions. In Internet-restrictive countries, "code" writers tend to shape the Internet as a means to promote a certain set of views and ideas—the ideology of the ruling class—and to exclude alternative or opposition ideas or views.

Drawing on this theoretical framework, this chapter examines the recent evolution of Internet filtering in Thailand, focusing in particular on the period following the September 19, 2006, coup and on the regulation of political content and communication. I address two main questions: (1) What are the major regulatory modalities in the Thai Internet filtering regime in the post-2006-coup era, and what are their major consequences for Internet stakeholders? (2) What are the reactions from civil society, and what mechanisms for addressing Internet filtering issues have emerged in Thailand?

The study relies on extensive analysis of laws and related policies, as well as in-depth interviews with stakeholders, policymakers, regulators, and members of civil society related to Internet regulation in Thailand. The discussion shows how the Internet in Thailand has turned into a contested terrain for competing values since the political change in 2006. What had been evolving as an emerging online public sphere became threatened and eroded in the postcoup years with the introduction of content-restrictive cybercrime law, an ID-enabled architecture, and the buttressing of a dominant social norm, which together constitute a schematic regulation by "code." However, civic groups and conscientious users who do not condone this controlling scheme have resisted it by projecting freedom and transparency as underlying values while challenging the legitimacy of Internet filtering and censorship through different means. While the contested nature of these Internet politics is not exactly equivalent to the color-coded politics that Thailand has been infamous for in recent years, there are definitely strong connections and shared implications.

Background

While Internet filtering has been actively practiced in Thailand since 2002, it did not become a political issue until after the military coup d'état of September 19, 2006.[8] The coup overthrew the highly popular Prime Minister Thaksin Shinawatra[9] and marked the beginning of a tumultuous chapter in Thai political history. In the aftermath of the coup, the self-exiled Thaksin and his red-shirt supporters have exploited the Internet as a primary channel for political communication.[10] Meanwhile, much political expression in Thailand has resorted to cyberspace, which has enjoyed relatively greater freedom of expression than have other forms of mass media. While broadcast media in Thailand have historically been controlled through state monopoly of the airwaves,[11] and print media generally had a lukewarm attitude toward the coup,[12] throughout the postcoup period (which international observers call color-coded politics for its red and yellow shirts), the Internet has emerged as a major public sphere.[13] Different online political forums, online newspapers, and political Web sites have become important platforms for expression, exchanges, and debates that represent a wide spectrum of political ideologies and orientations. As a result, authorities have increasingly zeroed in on Internet content as a target for censorship and surveillance in the post-2006-coup period.

Since September 2006, Thailand has seen four different governments led by four different prime ministers. The first postcoup PM was an appointee of the military junta, the Council for National Security (CNS), while the other three were MPs elected in 2007. The fourth prime minister—Abhisit Vejjajiva, leader of the Democrat Party, rose to power after the abrupt dissolution of the People's Power Party (PPP)[14] in late 2008, and the subsequent shift of alliance by a major faction in the preceding coalition government. The Democrat-led government, which was approved by the yellow shirts (the PAD) and the network monarchy, appeared to be brokered in by the military, and this alleged political illegitimacy was consistently used as a rationale by the United Front of Democracy against Dictatorship (UDD) in staging a series of protests against the Democrat-led government in 2009 and 2010.

In March to May 2010, when the red shirts took Bangkok in a protest calling for parliament's dissolution and a fresh election, the survival of the Abhisit government was again put to the test. Repeated negotiations failed to set an election date. The protests escalated into prolonged violent confrontations between the protesters and the military, and attempts to negotiate a ceasefire failed. More than 90 civilians and scores of soldiers were killed, with a total of more than 2,100 injured by the time the military successfully cracked down on the protesters on May 19. However, unrest rapidly spread throughout Thailand as red-shirt supporters clamored for justice. Many of these grievances were pouring out into cyberspace through social media where many dissidents were active.

Despite assuming office under unusual circumstances—over doubts regarding his government's sustainability and amid grievances against government mismanagement of the 2010 bloody crackdown—Abhisit completed his second year of administration with powerful backing still intact. In 2011 he was continuing to pursue his proclaimed goals of national reform and reconciliation.

To a number of observers and political experts, Thailand's wrenching political struggle over the past few years also boils down to another daunting question—the fate of the country after the end of the ailing 83-year-old King Bhumibol Adulyadej's reign. Other than the issues of support for Thaksin and the September 19, 2006, coup's legitimacy, Thai politics has also been polarized around loyalty to the monarchy. The right-wing conservatives and pro-status-quo forces in the military and current government, the main core of the network monarchy, are insecure and fearful of what will happen after the king passes from the scene.[15] During these dubious times, cases of lèse-majesté, involving prosecution of alleged insults to the immediate royal family, have dramatically increased. Critics see charges of lèse-majesté as an effective means to silence dissent, including on the Internet.

Insofar as online political communication is concerned, lèse-majesté has been the keyword in clamping down alternative viewpoints and in blocking Web sites related to Thaksin or the UDD (the red shirts). On more than one occasion, Abhisit and the Democrat-led government publicly announced that any lèse-majesté speech would not be tolerated offline or online. As part of their much-publicized policy to promote national reconciliation, the Abhisit-chaired cabinet approved a new agency in June 2010 to look after violations of the Computer-Related Offenses Act, in particular to protect and take care of the royal institution.[16]

This complex context is necessary for a nuanced understanding of the Internet-filtering regime in post-2006-coup Thailand. At least three regulatory elements can be delineated in this emerging filtering scheme: law, architecture, and social norms.

Law, Architecture, and Social Norms: Primary Regulators of the Thai Internet Filtering Regime

Law, architecture, and social norms are the dominant forms of regulation in Thailand's post-2006 Internet filtering regime. While Internet industry operators play a role, their regulatory influence emanates largely from the enforcement of law.

Law: Computer Crime Law and Lèse-Majesté

From September 2006 until the end of 2009, Thailand saw four different governments, two periods of massive political unrest, persistent insurgency, and an unprecedented

level of political polarization. In this highly volatile context, four major legal measures have been used to control online communication:

1. The Council for Democratic Reform's Order No. 5/2549 (2006)[17] on the Ministry of Information and Communication Technology's control of information disseminated through information technology systems (known as the CDR's Order No. 5).
2. The Computer-Related Offenses Act B.E. 2550 (2007).
3. The Emergency Decree on Government Administration in a State of Emergency B.E. 2548 (2005) and the Internal Security Act B.E. 2551 (2007).
4. Lèse-majesté provisions.

Since the CDR's Order No. 5 was enforced concurrently with martial law in the period immediately after the coup, it will not be discussed here.

The Computer-Related Offenses Act B.E. 2550 (2007)

The Computer-Related Offenses Act B.E. 2550, better known as the Computer Crime Law, was the very first legislation to be passed by the CNS-appointed National Legislative Assembly (NLA), an interim legislature after the coup.[18] Although the initial drafting of the law began in 1996, it was not actually passed until 2007, following an international controversy in April 2007 when the junta-appointed minister of MICT banned video clips deemed insulting to the Thai king and threatened to sue YouTube for carrying them. This threat of a lawsuit came after failed requests to YouTube to take down the problematic clips.[19]

Since its enactment, the computer crime law has been controversial, particularly its negative implications for online freedom of expression. Unlike conventional cybercrime law, which does not regulate content,[20] the Thai Computer-Related Offenses Act classifies content offenses committed on a computer as another major offense category in addition to offenses committed against computer systems or computer data. Section 14 of the law defines offenses as the import into a computer system of

- forged or false computer data, in a manner that is likely to cause damage to a third party or the public.
- false data in a manner likely to damage national security or to cause public panic.
- data constituting an offense against national security under the penal code; and pornographic data in a manner that could be publicly accessible.[21]

According to recently published research on online censorship through law and policy in Thailand, two major types of offenses can be delineated from prosecution charges filed under the 2007 Computer-Related Offences Act:[22] (1) offenses against computer systems or data and (2) offenses against content published online. Statistics in the three years since the new law came into effect show that 45 cases fall into the first

Table 5.1

STATISTICS OF OFFENSES CHARGED UNDER THE COMPUTER-RELATED OFFENSES ACT B.E. 2550 (2007) FROM JULY 2007 TO JULY 2010

Types of Offenses	Number of Cases	Percentage
Offenses related to computer system	45	24.32
Offenses related to content	128	69.19
Cannot be clearly categorized	12	6.49

Source: Suksri, Sawatree, et al., *Situational Report on Control and Censorship of Online Media through the Use of Laws and the Imposition of Thai State Policies* (Bangkok: Heinrich Böll Foundation Southeast Asia, 2010).

type (24.32%), 128 cases into the second type (69.19%), and 12 cases (6.49%) cannot be clearly categorized, as shown in table 5.1.

The data in table 5.1 show that the main emphasis in the enforcement of the new law is on content regulation rather than computer crimes that use computers as tools or aim at computer system as targets. National security is the main keyword for content offenses, most likely because it includes lèse-majesté (insulting the royal family), which is a taboo and a serious crime in Thai society.

The law also imposes severe sanctions for violators. For offenses against computer systems or computer data, the penalties include imprisonment of between six months and 20 years and/or a fine of between THB 10,000 (approximately USD 300) and 300,000 THB (approximately USD 9,036) while penalties for content offenses range from imprisonment for up to five years and/or a fine of up to THB 100,000 (approximately USD 3,012).[23]

Furthermore, the law grants broad powers to officials to investigate and gather evidence of a suspected offense committed by computer. Rather than suggesting the least intrusive action that will support their investigation, the law allows broad-based surveillance, censorship, and control of Internet-based activities. Competent officials, who are appointed by the minister of ICT, are authorized to do a range of things including summoning alleged parties to appear; requesting information and evidence; duplicating, decrypting, censoring, and accessing computer information; and confiscating or "freezing" computer systems.

In addition to granting these powers, the enforcement of the Computer-Related Offenses Act has important consequences for the regulation of Thai cyberspace, as follows:

1. *Legalizing blocking of Internet content*

Prior to the passing of the computer crime law, blocking of Internet content, which has been practiced since 2002 by the MICT, was always criticized for lack of legal

grounds. Critics have alluded to constitutional provisions that guarantee freedom of expression when attacking the blocking's illegality. For instance, the first clause in section 45 of the constitution reads, "A person shall enjoy the liberty to express his or her opinion, make speeches, write, print, publicize, and make expression by other means." The section goes on to prohibit the shutdown of media outlets like newspapers and broadcasting. While the Internet is never addressed in this constitutional provision, many cyber libertarians still see the Internet as a form of mass media that warrants the same protection. But with the passing and enforcement of the new computer crime law, blocking of Internet content is now legalized, falling as it does under the category of an offense. As section 20 of the law reads:

> In case the offences according to this law involve the publicizing of computer information that may have negative implications to national security as indicated in Part II of this law or as prescribed in 1/1 of the penal code or which may violate public order or good morals of the people, the competent officials, with approval from the appointed Minister, may petition, with supporting evidence, to the court within the jurisdiction, to halt the spread of such computer information.
>
> If the court issues an order to block the spread of information as in clause 1, competent officials may block the spread of that information themselves or request service providers to block the spread of that information.[24]

As a result, Internet filtering, which was a controversial issue in the past, is now considered legal. Since the act first came into effect, the MICT has applied section 20 to order thousands of Web sites alleged to contain lèse-majesté or pornographic materials to be blocked. Cracking down on lèse-majesté content has been identified as the MICT's policy priority.[25]

While the law specifies that a court warrant is mandatory, the actual enforcement has not been entirely strict. Based on interviews conducted as part of this study with selected Internet service providers, "requests for cooperation" from government agencies like the MICT and the Department of Special Investigation (DSI) do not always come furnished with court orders. The usual objectives of such requests are obtaining log files of Internet traffic, blocking problematic Web sites, and deleting problematic postings in online discussion forums. The requests often plainly make reference to provisions in the Computer-Related Offenses law, but without court orders. Although many service providers have qualms about blocking Internet content, they do not have any option but to comply.

2. *Indirect regulation via intermediary providers and self-censorship of online content providers*

The computer crime law enables the state to regulate intermediary providers who in turn regulate users. Section 15 of the law creates the burden of intermediary liability by imposing the same penalty on offenders as on intermediaries, regardless of prior

knowledge or intent. It claims that "any service providers [who] knowingly or unknowingly support or allow offenses indicated in Section 14 to be committed in the computer or system under his control *shall receive the same penalties as offenders under Section 14*"[26] (my emphasis).

According to the law, no distinction is made between network providers who act as mere conduits and content providers who actually host content in the way they are held liable for harmful or illegal content. Whether or not the providers have actual knowledge of the content in question or whether they quickly remove the content after becoming aware of it does not grant any immunity. However, the law does not extend liability to search engines and portals that provide links to illegal content.

Because of this intermediary liability enforcement, Internet intermediaries—network and content alike—have set up new measures to regulate content and in the process are passing regulatory constraints onto users. These measures are summarized in table 5.2.

Keeping a log file of Internet traffic is intended for investigation purposes, but the real target is the identity of users. In Thailand, where a civil registration system has been an inherent part of society for almost a century, it is relatively easy to pair IP addresses with citizen identification, since all service applications require the 13-digit citizen-identification number. While larger operators like Internet service providers (ISPs) can integrate this legal requirement into their existing operation, smaller providers—operators of Web sites, Web-hosting services, online discussion forums, and providers of institutional servers—have to set up some new form of identification and certification clearance system that makes users' network access conditional on providing credentials. In the case of Internet cafés, since they do not provide network service, customers are required to sign their names and citizen IDs in a logbook before using the service.

Meanwhile, medium to large organizational servers—academic institutions, companies, government agencies, and some Internet cafés—that provide Internet access

Table 5.2

SERVICE PROVIDERS' NEW REGULATORY MEASURES THAT CREATE INDIRECT REGULATION OF USERS AS A RESULT OF THE COMPUTER-RELATED OFFENSES ACT

New Content Regulation Measures Passed by Intermediaries Due to the 2007 Computer-Related Offenses Act
1. Keeping a log file of Internet traffic, including users' IP addresses, for 90 days
2. Identification and certification clearance requirement for users at institutional servers and for subscribers to online discussion forums
3. Installing filtering software at organizational servers to enable content filtering
4. Setting up a 24-hour monitoring system for online discussion forums
5. Incorporation of provisions of the law into codes of ethics/practice and terms of services

are increasingly installing filtering software on their systems, using a keyword or groups of keywords as criteria. Filtering criteria depend mainly on the policy of each organization, but the types of content offenses provided in the computer crime law are usually included.

Internet service providers also administer surveillance on interactive Web sites like online discussion forums and chat rooms that have registered IP addresses under their networks. For instance, CAT Telecom, a major ISP, administers this content-monitoring scheme through an in-house unit called Internet Data Center (IDC). An IDC staff member will periodically examine exchanges in online discussion forums, particularly political forums. If lèse-majesté content is found, IDC will inform the moderators of the particular online forum and give them 30 minutes to remove the content. If the content is not deleted within that time, CAT Telecom will block access to the IP address that hosts the online discussion forum.

As for operators of online discussion forums themselves, a 24-hour monitor of postings on the forum has been in place since the law came into force. While moderators of such forums make it part of their daily routine to remove illegal or harmful content, most feel reluctant and view the new law with much apprehension. The Web moderator of Prachatai (http://www.prachataiwebboard.com), Chiranuch Premchaiporn, who is now awaiting trial on intermediary liability charges filed under this law, described the main effect of the law being "a transfer of censorship from state agencies to webmaster, with the law as choker."[27] The late Somkiat Tangnamo,[28] webmaster of http://www.midnightuniv.org, admitted that he self-censored on lèse-majesté to an unprecedented level during the Abhisit government's rule. Evidently, self-censorship has become the prevalent practice for moderators of online forums, particularly politically oriented ones. See table 5.3 for a summary of such self-censorship/regulation practices during the post-coup period.

Although there has not yet been a study to examine online citizen reporters and their reaction to Internet filtering, related research shows that bloggers engaged in citizen journalism regulate content through codes of practice. In the case of OK Nation Blog, a popular journalistic blog, member bloggers develop their own sets of codes and practices, which closely observe provisions in the computer crime law and related laws like lèse-majesté.[29] In effect, legal provisions are incorporated into citizen reporters' codes and thereby become a framework for the self-regulation of bloggers.

The Emergency Decree on Government Administration in State of Emergency B.E. 2548 (2005) and the Internal Security Act B.E. 2551 (2007)

The Emergency Decree was passed in 2005 during the Thaksin administration, with the main objective of quelling the endemic insurgency in Southern Thailand. The

Table 5.3

SUMMARY OF SELF-CENSORSHIP PRACTICES IN ONLINE POLITICAL DISCUSSION FORUMS IN THE POST-2006-COUP PERIOD

Name of Online Discussion Forum	Self-Censorship/Self-Regulation Practices
www.midnightuniv.org	After lifting of the ban on the Web site in the days following the coup, the webmaster changed the site's comment-posting procedure by having all the posters send him an e-mail message rather than posting directly onto the forum so that he could filter all the postings firsthand. The practice, however, put off many regular visitors to the forum, which became a read-only forum without direct interaction among the forum users. Lèse-majesté has been the key criterion in monitoring postings, with particular sensitivity noted during the coup-installed government and the Abhisit Vejjajiva government.
www.prachathaiwebboard.com	Working staff have taken turns to maintain 24-hour monitoring of the forum to keep the postings under close watch, with lèse-majesté content a top priority. A distributed system of content monitoring was set up to enable Web moderators and users (with membership longer than one month) to mutually develop a watch list of problematic postings by flagging them. Web moderators look into the watch list and make final judgments about which postings ought to be deleted.
www.pantip.com* (Rajdamnoen room)	Webmaster installed a one-person-one-account regulation system in which each member has to register with a citizen ID number. Only registered members are eligible to post in the forum. This way, all members/posters know that they are traceable. Web site policy states that the Web moderator has the right to remove all postings regardless of direction (positive or negative) related to the royal family.

*www.pantip.com, or *pantip* for short, is a popular Web site that specializes in online forums. Its many forums and chat rooms encompass almost all topics of common interest, ranging from politics, science, sports, and fashion to entertainment. Its political online forum is named Rajdamnoen after a major thoroughfare in Bangkok where the Democracy monument is located and where many historic prodemocracy street protests took place. Transliterated in Thai, *pantip* means a thousand tips. The name derived from Pantip Plaza, a very famous computer mall in Bangkok.

Internal Security Act (ISA) B.E. 2551 was passed in November 2007 by the military-installed legislature—the NLA. The ISA establishes an Internal Security Operations Command (ISOC), directed by the prime minister and the commander-in-chief of the army. The ISOC has the power to have relevant government officials implement any action or withhold the implementation of any action.

Both laws have imposed far-reaching restrictions on the right to free expression, peaceful assembly, and freedom of movement, and the right to a fair judicial process. During the political turmoil in April 2009, both laws were invoked on more than one occasion in certain districts of Bangkok during demonstrations by the United Front of Democracy against Dictatorship (UDD). The enforcement of these laws enabled the MICT and other government agencies to exercise broad-based censorship and surveillance of the media, including the Internet.

During the "Red Shirt Protests" from April to May 2010, a significant number of red-shirt sites were targeted and blocked, following a block list issued under the Emergency Decree that ordered 36 Web sites to be filtered. During this period ONI conducted tests on two major ISPs—state-run TOTNET and TRUE, a private telecommunications conglomerate. The testing found blocked sites under common content categories in both ISPs as follows: free expression and media freedom, gambling, political reform groups, and social networking. However, TOTNET was found to have filtered almost twice the number of sites (29 URLs) than TRUE and more content categories. For example, anonymizer and circumvention sites were blocked by TOTNET but not by TRUE. Significantly, neither TRUE nor TOTNET filtered the entire block list, with TOTNET blocking only 10 URLs from the list and TOTNET filtering this same set and an additional 13 for a total of 23 URLS.[30] Meanwhile, community radio stations and cable television stations were raided, and satellite television stations' signals were cut off.[31] While it is in effect, the Emergency Decree supersedes all other laws. It has been attacked by critics as an authoritarian piece of legislation that allows unprecedented state control.

Lèse-Majesté Provisions

Lèse-majesté—damaging or defaming the king and royal family—has been the single offense most frequently applied by the Thai authorities against Internet users and service providers under the computer crime law, largely because of the postcoup political crisis. Lèse-majesté provisions in Thai law include sections 8 and 9 of the 2007 constitution and section 112 of the penal code. Section 8 of the 2007 constitution notes that "the King shall be enthroned in a position of revered worship and shall not be violated. No person shall expose the King to any sort of accusation or action."[32]

Lèse-majesté is also classified under Offenses Relating to the Security of the Kingdom in Thailand's penal code. It has always been part of the code and rarely subject to change since its inception in 1957. Thai authorities treat lèse-majesté as a matter of national security, and cases of lèse-majesté usually entail severe punishment. This fact is evident in section 112 of the penal code, which reads, "Whoever defames, insults, or threatens the King, the Queen, the Heir-apparent or the Regent, shall be punished with imprisonment of three to fifteen years."[33] The royalist Democrat government, which has ruled since late 2008, recently proposed to Parliament a legal amendment that will raise prison sentences for lèse-majesté to a maximum of 25 years. The amendment will also add a maximum fine of one million baht (about USD 28,500). Currently, lèse-majesté carries no fine.

An analysis of legal prosecutions related to Internet content since the 2006 coup shows that lèse-majesté was the leading offense. When bringing charges of defaming the monarch on the Internet, the police will usually cite section 14 of the computer crime law together with section 112 of the penal code, since the offense is covered by provisions in both pieces of legislation. See table 5.4 for analysis of prominent cases of Internet content offenses during the post-2006-coup period.

Of all the content offenses charged, the only unresolved case is that of Chiranuch Premchaiporn, webmaster of Prachatai. The interesting point about Chiranuch's case is that she was first charged with only the computer crime law under an intermediary liability charge because the alleged lèse-majesté comment was posted by a forum user and not by herself. However, in September 2010 she was arrested on multiple charges including lèse-majesté for an interview published on the Web site in 2008 with a man who was arrested and charged with lèse-majesté for refusing to stand up during the royal anthem in a movie house.[34]

It should be noted that lèse-majesté cases have also increased offline. From 2008 to 2009, at least four cases were charged, alongside those in cyberspace:

- A local man, Chotisak Onsoong, went to a movie and refused to stand up while the royal anthem played before the movie. He was later arrested after the movie operator reported him to the police for an act deemed an insult to the king.[35]
- An Australian man, Harry Nicolaides, was arrested and sentenced to three years in prison for having published a book that defames the crown prince.[36] He later received a royal pardon and was immediately deported to Australia.
- Political science professor Giles Ungpakorn was summoned for questioning for an alleged lèse-majesté charge. He later fled to England, for fear of not getting a fair trial.[37]
- Political activist Daranee Chancheongsilapakul, also known as Da Torpedo, was convicted of lèse-majesté and sentenced to a combined jail term of 18 years. Daranee reportedly made a series of inflammatory speeches against the king and the 2006 coup at one of the red-shirt political rallies.[38]

Table 5.4

SUMMARY OF LEGAL CASES AND OFFENSES RELATED TO INTERNET CONTENT DURING THE POST-2006-COUP PERIOD

Date of Incident	Type of Offense Allegedly Committed	Summary of Incident	Legal Measures Taken
September 2007	Lèse-majesté (section 8 of the constitution, and section 112 of the penal code); input into a computer system of data that were an offense against national security or terrorism according to the criminal code [section 14(3) of the Computer-Related Offenses Act]	An alleged lèse-majesté comment against the monarchy on the now-defunct political forum Web site www.propaganda.forumotion.com by a man using the pseudonym of Praya Pichai. The man was brought into custody and jailed for two weeks but charges could not be filed for lack of evidence.	The Web site was shut down and Praya Pichai faced ten years of continued surveillance and a threatened prison term if he posts a political comment online again.
April 2008	Input into a computer system of pornographic computer data that are accessible to the public [section 14(4)] of the Computer-Related Offenses Act	Owner of 212 café online forum was arrested for hosting a link to a pornographic Web site. At the arrest time, the police could not specify the problematic URL of the link. Although the forum webmaster immediately shut down the Web site, a month later, the police raided his home office and appropriated his servers and computer devices.	The forum owner was summoned to appear at a police station and to submit the names and contact list of all the forum's clients (about 28,000 people). He eventually spent one night in jail and later posted bail for THB 100,000 (USD 3,250).
January 2009	Lèse-majesté (section 8 the constitution, section 112 of the penal code), input into a computer system of computer data that is an offense against national security or terrorism according to the penal code [section 14(3) of the Computer-Related Offenses Act]	A blogger was arrested and convicted for having uploaded royally defaming materials on the www.youtube.com Web site. He was held in custody for three months before a lèse-majesté verdict was announced in April, resulting in a ten-year imprisonment. In June 2010 his petition for a royal pardon was answered and he was released from prison.	The police (through the high-tech crime unit and DSI) kept the convicted blogger on surveillance for about six months before the arrest.

Continued

Table 5.4

(continued)

Date of Incident	Type of Offense Allegedly Committed	Summary of Incident	Legal Measures Taken
March 2009	Intermediary liability or consent/ negligence of operators for offenses to be committed (section 15 of the Computer-Related Offenses Act)	Webmaster of the independent online newspaper www.prachatai.co.th was arrested because alleged lèse-majesté comments were posted on the Web site's online discussion forum at www.prachataiwebboard.com—though she said that she had removed them immediately after the first notice from the police. She is currently undergoing trial.	Prior to the arrest, Prachathai had reportedly received "requests" from the military to remove from its Web site articles and commentaries on the monarchy and the military.
November 2009	Import of false computer data that could threaten national security or cause public panic [section 14(2) of the Computer-Related Offenses Act)	Two brokers were arrested for having posted information on two political online forums—www.prachataiwebboard.com and www.sameskyboard.org. One of the postings was a translation of a Bloomberg news service article on a rumor about the king's deteriorating health. The postings allegedly helped the market to plunge 7 percent during trading on October 14 and 15, 2009. However, the webmaster of www.prachataiwebboard.com contradicted the police theory that the two brokers were helping spread the rumors for financial gain by confirming that both were long-standing members of the forum.	High-tech crime division and DSI have been keeping both political forums under constant surveillance throughout the postcoup period. When the suspects were arrested, their apprehension was in the context of a stock market manipulation. But a police official in charge did mention that their spreading of rumors took place on "two politically problematic and controversial Web boards."

Table 5.4

(continued)

Date of Incident	Type of Offense Allegedly Committed	Summary of Incident	Legal Measures Taken
September 2010	Lèse-majesté (section 112 of the penal code); inciting unrest by publication (section 116 of the penal code); input into a computer of system computer data that are an offense against national security or terrorism according to the penal code [section 14(3) of the Computer-Related Offenses Act]; and intermediary liability or consent/ negligence of operators for offenses to be committed (section 15 of the Computer-Related Offenses Act)	Webmaster of www.prachatai.co.th was stopped at an immigration checkpoint and arrested at Bangkok International Airport after returning from the Internet at Liberty 2010 conference in Budapest, Hungary. Her arrest warrant was based upon an interview published in www. prachatai.co.th about a man who was charged with lèse-majesté for failing to stand up for the royal anthem in a movie theater in 2008.	The arrestee was bailed out on THB 200,000 (USD 6,600) bail. She was expected to report to Khon Kaen provincial police station, where the arrest warrant was issued, once a month until the case is either dismissed or filed to the public prosecutor.

Architecture: From Automatic URL Filtering to an ID-Enabled Cyberspace

Automatic URL Filtering

After the September 2006 coup, the MICT was faced with mounting complaints over lèse-majesté cases, which were reportedly mushrooming on anticoup and pro-Thaksin Web sites. The existing IP-based filtering at ISP levels, based on block lists circulated by MICT, was deemed ineffective and was also criticized for overblocking. The interim minister of ICT thus revisited the idea of an automatic Internet filtering system, which was discussed in the later years of the Thaksin administration but did not materialize. As a result, a feasibility study was carried out, and a pilot project was commissioned to local researchers. The new automatic filtering system was installed at the level of international Internet gateway (IIG),[39] which is a higher level of networking than national Internet exchange (NIX) or ISPs.[40] All IIGs under CAT Telecom Plc were the first to be installed with the new automatic filtering system, since CAT Telecom is a state enterprise and reports directly to the MICT. The filtering technology was developed by a group of computer-engineering researchers at the Bangkok-based Kasetsart University. The URL filtering technique was originally developed to filter out unwanted content such as spam but could also be used to filter Web access by blocking at application layers or at URL levels.[41] The system began a trial run in 2008 and has been fully operational since early 2009.

Essentially, the URL filtering technique uses what Robert Faris and Nart Villeneuve call proxy-based filtering strategies.[42] Internet traffic passing by the filtering system is reassembled, and the specific HTTP address being accessed is checked against a list of blocked URLs or blocked keywords in the URL. When users attempt to access these URLs, they are subsequently blocked. But instead of showing an MICT block page indicating that the site has been blocked (as would be the case of IP blocking at ISP level), the new system has created a block page that looks like the browser's default error page, possibly to disguise the fact that the government is blocking these sites.

ID-Enabled Cyberspace

Largely because of enforcement of the computer crime law, online service providers (OSPs)—those that host social networking services, blogs, and Web sites—have increasingly set up a system that enables "traceability regulation."[43] To access content and services on these Web sites, users are required to provide some sort of identification or certification first. Using traceability regulation as a framework, we surveyed popular local online services like online discussion forums, blogs, social networking services, portals, and online newspapers. The results are shown in table 5.5.

Table 5.5

IDENTIFICATION AND CERTIFICATION REQUIREMENTS OF SELECTED ONLINE SERVICES

	Identification/ Certification upon Login	Identification/Certification upon Registration			
Type/Name of Web site	User Name/ Password	E-mail	13-Digit Citizen ID	Name/ Address/ Phone	Remark
Online discussion forums					
pantip.com	√	√	√	√	Member registration requires citizen ID and a personal photo
mthai.com	√	√			
forum.serithai.net	√	√			
Blog					
blogging.com	√	√	√	√	Membership bundled with that of pantip.com
exteen.com	√	√	√		
oknation.net	√	√	√	√	Member registration requires citizen ID and a personal photo
blogger.com	√				Login via Google account
gotoknow.org	√	√		√	Member registration requires real name
asiancorrespondent .com	√	√			English-language blog. Covers politics and situation in southern part of Thailand. Provides analyses of news from the *Bangkok Post* and *The Nation.*
Social networking service (SNS)					
facebook.com	√	√			

Continued

Table 5.5
(continued)

Type/Name of Web site	Identification/ Certification upon Login: User Name/ Password	Identification/Certification upon Registration: E-mail	13-Digit Citizen ID	Name/ Address/ Phone	Remark
Twitter.com	√	√			
Hi5.com	√	√			
MySpace.com	√	√		√	Member registration requires name and birth date
Portal					
hunsa.com	√	√	√	√	Does not require citizen ID. User will be entered into "lucky draw" and able to join online auction if citizen ID is provided.
sanook.com	√	√			
kapok.com	√	√			
th.yahoo.com	√	√		√	Member registration requires name and birth date
Online newspaper					
thairath.co.th	√	√	√	√	Membership is required to search historical news
manager.co.th	√	√		√	Member registration requires name, birth date, and postal code
posttoday.com	√	√			Member registration requires name and birth date

Table 5.5
(continued)

Type/Name of Web site	Identification/ Certification upon Login: User Name/ Password	Identification/Certification upon Registration: E-mail	13-Digit Citizen ID	Name/ Address/ Phone	Remark
komchadluek.net	√	√	√	√	Membership is required to receive e-newsletter and to post comments on the news
Others (video and photo sharing, satellite TV)					
voicetv.co.th	√	√		√	Member registration requires name and birth date
youtube.com	√	√			Can watch and upload video clips
flickr.com	√	√		√	Automatically registered with Yahoo account

The most minimal forms of identification and certification required in all surveyed OSPs are user name and password for logging into the system. For registration, all providers require an e-mail address as a precondition for access, while some require name, address, and phone number, and a few require the 13-digit citizen identification number. In any case, it is apparent that an architecture of identification has been established in the Thai cyberspace as a result of the new computer crime law.

Social Norms: A Benevolent and Inviolable Kingship

While lèse-majesté may sound peculiar to non-Thais, it has been a deep-seated concept in Thai culture for centuries. The monarchy has always been a central institution in Thai society. Despite the 1932 revolution that changed the governing regime from absolute monarchy to constitutional monarchy, the king was still allowed to exercise sanctioning prerogatives of legitimization. At that time, the first constitution was regarded as a royal gift, while the throne was generally viewed as holding a position

of moral superiority over the new political leadership. This view still appears to prevail today.

In past and present constitutions, the monarch, as the head of state, has these privileges:

1. He is to be unreservedly respected: his person is inviolable, and he is not subject to the jurisdiction of the courts.
2. He is the Head of the State.
3. He is the soul of the nation and the font of national harmony.
4. He is above politics.
5. He is politically neutral, without aligning with any political group or party.
6. He can do no wrong (constitutionally).

Furthermore, the Thai conception of kingship is a combination of the Hindu divine right of *deva raja* and the Buddhist patriarchal kingship in which the king rules according to the law or dharma. Therefore, the legitimacy of the monarch is derived not only from divine right but also from his own conduct and commendable deeds. The present king, Bhumibol Adulyadej, who is now the world's longest-reigning monarch, has been credited for his lifelong dedication to rural development and the livelihoods of his poorest subjects. He is thus well loved and respected by the general Thai public. In 2006 on the 60th anniversary of his coronation, the entire country glowed yellow as loyal supporters of the king donned special yellow royal shirts in celebration everywhere throughout the year.

With exceptional privileges, conceptual dominance, and public reverence, the Thai monarchy has been used as a source of legitimacy in Thai politics. A former prime minister (1957–1963) and military dictator, Field Marshal Sarit Thanarat, made extensive use of the monarchy to legitimize his regime both domestically and internationally. This legitimization often happens at the expense of free speech. In the past, dissidents who were charged with lèse-majesté were usually social critics or those who openly resented military involvement in politics. Meanwhile, filers of lèse-majesté suits were typically from the military.

Traditionally, the monarchy has been identified as one of the core values to be protected under national security, which includes three things—the monarchy, religion (Buddhism), and the Thai nation. Any attempt to undermine these so-called three pillars of Thai society would be viewed as a threat to national security. As these core values are usually fused together, it is not uncommon for a show of disrespect, including criticism of the king, to be interpreted as "unpatriotic."

There has always been tension between free speech and royalism in Thailand, but never has the anxiety been so great as in the age of the Internet and a time of foreseeable royal succession. With the borderless and robust nature of the Internet, it is no longer feasible to keep the king virtually beyond criticism in the virtual world. But no

matter how futile and ultraconservative lèse-majesté filtering may appear to some liberal people, there are those who support it and even participate in monitoring Web sites and reporting lèse-majesté to authorities. Statistics released by the MICT show that the greatest number of complaints received on Internet content had to do with lèse-majesté.[44]

Reaction from Civil Society and Mechanisms for Addressing Internet Filtering

In response to Internet filtering issues, members of civil society have reacted in a number of ways and used varying strategies to deal with new regulatory constraints. Members of civil society also contest what they conceive to be the government's abuse of power and violation of free speech online.

Online Security Caution

According to interviews with selected civil society activists, tightening up security in their online use seems to be the top strategy in coping with authorities' censorship and surveillance. This approach was manifested most frequently in their technological choice. For instance, a few Internet advocacy activists said they deliberately gave up the more popular Windows platform and opted instead for Linux as an operating system. Some also chose to disable the conversation-recording feature of Gtalk and turn on the secure access feature (SSL) in Gmail. The majority are very cautious about their passwords. Not only do they keep their passwords as their most confidential information, but they also change passwords frequently. Their choice of password is also crucial. One online activist said he avoided words in the dictionary and used multiple layers of password protection. In using social media like Facebook or Twitter, a few activists noted that they exercise more caution in accepting friends or in setting the circle to which their personal information will be accessible. Similarly, in using online discussion forums, these activists are careful in posting comments and in registering their personal information to the Web sites. Usually, they do not give anything beyond their e-mail address to avoid being identified.

Evasion and Circumvention

When it comes to Web censorship, a number of users wishing to access blocked Internet content can find easy ways around it by using proxy or VPN or using Google translate or Google cache. But with Web 2.0 applications and social media, things are a bit more complicated to get around. At this level, OSPs that rent out server space to a large number of Web site developers and operators of social media platforms are becoming increasingly important as intermediary censors for online content. Ethan

Zuckerman refers to OSPs' role in Internet filtering as "intermediary censorship."[45] They have become important choke points for Web users who publish content on Web servers they do not control. Such censorship is observed in at least three online political discussion forums that the research team studied in the postcoup period. These findings are summarized in table 5.6.

The summary in table 5.6 clearly shows that because a number of smaller Internet providers rely on them to publish content, OSPs can be powerful entities in controlling online speech. But the same summary also shows that this newer generation of Internet publishers is savvy enough to circumvent such intermediary filtering systems by exploiting alternative hosting services overseas. While this strategy may not solve their problem entirely—since the state can still block through URL-filtering at the IIG level—it still suggests that cyber citizens make efforts to redress the problem with whatever technological options are available.

Campaigning for Local and International Support

Based on interviews with civil society members, their most immediate concern about Internet filtering in Thailand is the new computer crime law. To them, the new law is more of an effort by the after-coup government to curb threats against national security and the monarchy, rather than to stop cybercriminality. In response to arrest cases under this very law, several rights-based groups have campaigned in support of the arrestees. The most obvious case is that of Chiranuch Premchaiporn, who has been arrested twice with charges under the same law. (See details about Chiranuch's arrest in table 5.4.) Because Chiranuch is a member of the prominent online freedom advocacy group—the Thai Netizen Network (TNN)[46]—her case has been continuously reported in Prachatai (until it was blocked by the emergency decree during the red-shirt crisis of March to May 2010) and in other alternative online media including mailing lists of TNN. Ever since Chiranuch's first arrest in March 2009, campaigns to support her and Internet freedom, using her case as a rallying point, have been growing steadily.

First, only the TNN and alliance organizations like Campaign for Popular Media Reform (CPMR)[47] and Freedom against Censorship Thailand (FACT)[48] joined forces. Gradually, other local human rights nongovernmental organizations (NGOs) joined the campaign to free Chiranuch (also known by her nickname Jiew) by submitting an open letter seeking the immediate dropping of charges against her and dissuading public prosecutors from pursuing trial. These include the Network of Human Rights Lawyers, the Project on Legal Environment, and the Association for Civil Rights and Liberties. Subsequently, the circle grew to more regional participation with the Southeast Asian Press Alliance (SEAPA), Southeast Asian Media Legal Defense (SEAMLD), which is a regional spin-off from the global Media Legal Defense Initiative (MLDI),

Table 5.6

SUMMARY OF ONLINE SERVICE PROVIDERS' ROLE AS INTERMEDIARY CENSORS OF ONLINE DISCUSSION FORUMS IN THAILAND

Name of Online Discussion Forum	Intermediary Censorship Experience	Reaction
www.midnightuniv.org*	The Web-hosting company from which the forum rented server space was blocked during the aftermath of the coup and discontinued service to the forum thereafter.	Forum moderator decided to change to a new Web-hosting company and introduced a new filtering system for forum postings.
www.prachataiwebboard.com†	During the period of intense political conflict in 2008–2009, the contracted Web-hosting company decided to terminate service to the Prachatai online forum, evidently out of fear of the political sensitivity of the forum's content.	Webmaster decided to separate hosting services used for the online newspaper and for the online political discussion forum. The latter moved to rent from an overseas Web-hosting service, to avoid blocking problem.
www.sameskyboard.org‡	The contracted Web-hosting service company was reportedly pressured by the MICT to abruptly halt service for www.sameskybooks.org/ and its other online services. The MICT's interference also wiped out the affiliated online forum—www.sameskyboard.org—and all the database kept by the online publisher for the previous five years.	The editor of the www.sameskybooks.org/ publicly condemned MICT for their alleged interference and opened a temporary Web site and a new online forum. Later, the service shifted to an overseas hosting company for all its online services.

*The site www.midnightuniv.org, known as Midnight University, is a leading alternative educational Web site that compiles academic resources on various sciences including social science and anthropology. The site also provides a forum for the public to exchange opinions on matters of interest. A group of progressive-minded academics, a number of whom are from Chiang Mai University, run this Web site and the political discussion forum attached to it. After the 2006 coup, www.midnightuniv.org attracted a lot of media attention because it represented very rare voices in society that condemned the coup and denounced the postcoup (2007) constitution.

†The site www.prachatai.co.th, or Prachatai for short, is an online newspaper that is very famous for its leftist and highly critical political standing. Prachatai is also openly anti-2006-coup. Founded in 2004 by a well-known social activist, it aims to be an independent medium free from state control, after the model of the famous Minda News (http://www.mindanews.com) in the Philippines. Prachatai's initial funding was allocated by the Thai Health Promotion Foundation. Later, when the foundation blacklisted it for probing into the foundation's spending, its supporter shifted to overseas sources such as the Rockefeller Foundation and Open Society Institute. Prachatai also runs a famous left-wing online discussion forum—www.prachataiwebboard.com, of which the political room is most popular.

‡The site www.sameskyboard.org, or samesky for local users, is a popular left-wing online political discussion forum attached to www.sameskybooks.com, an online site of local publishers of *Samesky* magazines. *Samesky* magazine is well-known for its progressive and critical viewpoints on politics and society.

and Asian Human Rights Commission (AHRC), among others. At the time of writing (October 2010), a global campaign to support Chiranuch was well under way, with leading media advocacy and human rights organizations such as the Electronic Frontier Foundation (EFF), Committee to Protect Journalists (CPJ), International Court of Justice (ICJ), Open Society Institute (OSI), Human Rights Watch (HRW), and Amnesty International involved. These organizations' main criticism is directed at Thailand's censorship policy and its impact on human rights and free speech, especially in cyberspace. Both the new computer crime law and lèse-majesté have been criticized as tools to suppress dissent and persecute political opponents.

After Chiranuch's second arrest in September 2010, a wider circle of Internet users promoted her cause through social media. Examples include a campaign using "free jiew" as a tag on the popular micro-blogging site Twitter (https://twitter.com/search?q=%23freejiew); blogs dedicated to the cause (http://freejiew.blogspot.com); and a platform set up by Digital Democracy to receive donations in support of her bail (http://digitaldemocracy.chipin.com/free-jiew).

Public Advocacy and Policy Lobbying

Alongside campaigning for support at local and international levels for Chiranuch's case, civil society organizations have also been active in advocating for public awareness about Internet restrictions in Thailand. In fact, advocacy work through public education has been the core work of the TNN, of which Chiranuch is a founding member. For the past two years, TNN has been at the forefront in organizing meetings, seminars, and public forums on issues related to Internet freedom. For instance, in August 2010, TNN, together with Media 4 Democracy and SEAPA, organized a high-profile seminar on the Computer-Related Offenses Act, on its third anniversary. A former information minister, an online newspaper webmaster, a popular blogger, a media watch representative, and Chiranuch herself shared comments on the computer crime law's impact on democratization in Thailand. The common sentiment is that restrictive law and careless enforcement during political polarization will contribute negatively to democracy because self-censorship becomes the rule for safety, hence deterring debate and the climate of opinion that are so fundamental to democracy.

In addition to public education, civil society has also used policy lobbying as another avenue to redress Internet control issues. In early 2009, several rights groups, including TNN, CPMR, and FACT, submitted an open letter to current Thai Prime Minister Abhisit Vejjajiva demanding an amendment of the computer crime law to make it more transparent and less politically motivated. Although Abhisit stressed civil liberties in his inauguration speech in December 2008, he has ruled out a repeal of the computer crime law.

Ambivalence and Indifference

In contrast to the stance and strategies taken by NGOs and activists, key institutional bodies responsible for human rights in Thailand are not only slow in responding to complaints about impediments to freedom from enforcement of the new computer law, but they have also been ambivalent in the face of lèse-majesté and the protection of national security. According to the chairperson of the National Human Rights Commission (NHRC), a post-1997 reform independent organization, the MICT's Internet blocking is a new challenge for many organizations, including NHRC. There are still few complaints at NHRC about Internet filtering as a violation of the freedom of expression—compared to other more pressing issues such as exploitation of natural resources, abuse of power, and governmental malpractice. The complicated nature of the Internet has also contributed to Thai institutions' limited understanding of the seriousness of the situation.

The NHRC usually refers ICT-related complaints, including online blocking, to the National Telecommunications Commission (NTC), an independent telecommunications regulator and now interim regulator of broadcasting. While acknowledging that violations of freedom do exist on the Internet, the NHRC also admitted they lack the necessary technical and legal expertise to deal with the problem.

Apart from the NHRC, another avenue where people can address Internet filtering issues is through human-rights-related commissions attached to the House of Parliament and the Senate. However, an interview with one chairperson of such a commission—the House commission on human rights, freedom, and consumer protection—revealed a rather conservative stance. Absolute freedom, this person argued, can threaten national security, especially when it involves the monarchy. The reverence of the monarchy, he stressed, is unique to Thai society and shall not be compromised at any cost. In this light, the new computer crime law is a justified effort by the government to properly regulate Internet use by balancing freedom of expression with national security. The chairperson feels that the judicial system is always open for online civil rights groups to tap if the rights to communicate and freedom of expression online are violated by the law.

Conclusion

At a glance, the politics of Internet filtering in Thailand may only reflect the larger political struggle between pro- and anti-Thaksin forces or between pro- and antimonarchy forces. But a closer examination yields another type of politics beyond the dominant color-coded politics. This politics of the Thai Internet code involves a subtle relationship between different elements in the regulation of Thai cyberspace.

In the post-2006-coup experience, the Computer-Related Offenses Act of 2007, a product of the coup-installed legislature, appears to be a major driving force in shaping the cyber experience in Thailand. A number of new regulatory practices have resulted, including the following:

- Legalizing of blocking at network levels.
- Indirect regulation by intermediary providers, which gave rise to intermediary censorship by online service providers and self-censorship of online content providers.
- Creating an ID-enabled architecture that promotes traceability regulation.
- Incorporating censorship into the cyber community's code of practice.
- Self-censorship by users in the online public sphere.

Other laws such as the Emergency Decree, the Internal Security Act of 2007, and lèse-majesté laws also help intensify regulatory restraints with the elements of surveillance and punishment. Gradually, Internet operators—network, service, and content—and Internet users in Thai society have learned to integrate these legal provisions into their cyber behavior. While it is true that lèse-majesté law has been in existence since 1957, its actual enforcement or looming possibility of enforcement has never been as evident as in the present period. I for one still remember the early days of the Internet in the early 1990s in which Thai Net users exchanged opinions on the future of the monarchy on Bulletin Board Service (BBS) using anonymous e-mails. The Internet was free and unregulated because it was difficult to identify the user or poster of comments. This is no longer true in Thai cyberspace, since everyone is now visible and traceable through the new ID-enabled architecture.

Notably, the increased transparency of the Thai Internet is made possible by indirect regulation from the new law. As users are forced to give self-authenticating facts to service providers in order to gain access to the Net, they have contributed directly to the regulation of their own behavior in cyberspace. The new law has changed the regulation of architecture through design constraints that condition netizens' access to cyberspace.

Meanwhile, automatic URL filtering, which involves more subtle filtering design than IP blocking, has also led to a greater technical capability to deny access to information resources while reducing the possibility of blockers being discovered. Though not directly related to the new law, this new technological design has indeed made filtering more malleable and more effective.

The law and the architecture aside, social norms also have a powerful role to play in the Thai politics of Internet filtering. The respect and reverence for the monarchy, particularly for the current king who has reigned for more than 62 years, is a deep-rooted norm in Thai society. Whether lèse-majesté is legitimate or not may be a moot point. What is clear is that this enigmatic norm carries with it high sensitivity in cyberspace as well as in the "real" world. Alongside the increase in prosecution cases

related to lèse-majesté speech online and offline, there has also been growing evidence of participatory forms of censorship—by service providers, content operators, and users—against lèse-majesté. While this participatory censorship is partly a consequence of the climate of fear arising from the new computer law and strict enforcement of lèse-majesté law, the law is not an isolated cause. After all, as Lessig rightly notes, norms constrain through the stigma that a community imposes, while law constrains through the punishment it threatens. In the Thai scenario, both elements apply.

Post-2006 Thailand is an interesting time and place to study Internet censorship and control. In this unique context, an ideological struggle is being played out between the old norm of preserving the sanctity of a revered institution that unites the nation and the new norm of free speech that could disrupt national order. If this ideological contest continues, we are likely to see more filtering, more cyber surveillance, more cyber policing, and more "rule of law" being used to suppress and undermine human rights and free speech online. In the meantime, civil society will employ more tools and options to circumvent politically motivated censorship through wider and higher circles of advocacy, to ultimately prove that freedom is not a crime.

Notes

1. Reporters Without Borders, "Is Thailand a New Enemy of the Internet?" January 12, 2009, http://en.rsf.org/thailand-is-thailand-a-new-enemy-of-the-12-01-2009,29945.

2. This was a result of the 1997 reform-oriented constitution that promoted transparency, accountability of government, and people's rights, liberties, and participation.

3. The Ministry of Information and Communication Technology (MICT) was set up as part of the bureaucratic reform introduced by Thaksin Shinawatra, then the new prime minister. From its inception, the MICT's main policy has been Internet regulation. This began with introducing filtering through the unit called "Cyber-inspector," aimed largely at pornographic content. Later in 2003, the MICT passed regulatory measures to regulate online gaming in response to moral panic in Thai society.

4. The "red shirts" is the informal name for the United Front of Democracy against Dictatorship (UDD), a major political organization in the post-coup period. Members of the UDD are known for wearing red clothes during antigovernment protests. Established in 2006 as Democratic Alliance against Dictatorship (DAAD), the main objective of the red shirts then was to fight against its arch rival—the People's Alliance for Democracy (PAD)—and to support the ousted former Prime Minister Thaksin Shinawatra. Supporters of the UDD are largely rural grassroots people who benefited from Thaksin's populist welfare policy, but also include the urban middle class who admire Thaksin's business-oriented administrative policy and action.

5. Duncan McCargo, "Political Outlook: Thailand," *Regional Outlook* (2010–2011), 54–58.

6. The People's Alliance for Democracy (PAD) originated from the mass movements preceding the September 2006 coup that ousted Thaksin from the premiership. The PAD, also known as the yellow shirts, spent much of 2008 protesting against two successive Thaksin-nominated governments—led by the late Samak Sundaravej and Somchai Wongsawat (Thaksin's brother-in-law)—that arose from the December 2007 election. The PAD's 190-day protest in 2008 was marked by the seizure of the Government House and the Suvarnabhumi International Airport in Bangkok, which had devastating and lasting effects on the Thai economy. In 2009, leaders of the PAD entered electoral politics by establishing the New Politics Party.

7. Lawrence Lessig, *Codes and Other Laws of Cyberspace* (New York: Perseus, 1999), 15–30.

8. This coup took place after a 15-year interval. The previous coup was staged in 1992 by the so-called National Peace-Keeping Council (NPKC), led by then Supreme Commander-in-Chief General Sunthorn Kongsompong. The NPKC overthrew General Chatichai Choonhavan, a civilian prime minister, who led a coalition government for less than two years.

9. Thaksin Shinawatra, founder of the Thai Rak Thai (TRT) Party, was a famous telecommunications tycoon, having made his fortune from satellite and mobile phone concessions through Shin Corporation. Thaksin was also a popular political leader who led the longest democratic and civilian rule—six years—in contemporary Thai history. Thaksin's popularity was largely attributed to populist policies that featured income redistribution, cheap health care, microcredit schemes, and many policy innovations in support of globalization and neoliberal economy. Thaksin is not well liked by a large number of urban or middle-class voters who are repulsed by his arrogance, authoritarian tendencies, and policy discrepancy while in power. He was also widely accused of disloyalty to the crown, an accusation that was largely used as a justification for the September 19, 2006, coup.

10. For instance, Thaksin reportedly launched and managed www.thaksinlive.com on his own before moving on to social media like Facebook and Twitter with http://twitter.com/Thaksinlive, in addition to making periodic video-linked appearances via satellite at the red-shirts' rallies. In late 2009, his family launched an Internet television site called Voice TV, which can be accessed on the Web at http://www.voicetv.co.th.

11. Up until 2001 when the first community radio station aired, all broadcast frequencies—524 for radio and six for national television stations—were controlled by state agencies. Major controllers of the airwaves include the Department of Public Relations (PRD), the Mass Communication Organization of Thailand (MCOT), and the Ministry of Defense, mainly through the army.

12. The Thai printed press, which has always been an important institution in shaping public opinion and setting public agenda, came under heavy criticism for condoning the coup. Notably, three leaders of professional media organizations/associations were appointed by the junta to be in the National Legislative Assembly (NLA), an interim legislature. Also, the printed media were able to push for the passage of a liberal print notification law to replace the draconian and authoritarian print law during the NLA term.

13. According to a nationwide survey of Internet users in 2009 by the National Electronics and Computer Technology Center (NECTEC), Thailand has 18.3 million Internet users, of which 1.8 million are broadband users.

14. The PPP shared the same fate as its predecessor—the TRT Party—when it faced dissolution by a ruling from the Constitutional Tribunal in November 2008 over charges of election fraud.

15. Thitinand Pongsudhirak, "The Search for a New Consensus," *Journal of International Security Affairs,* no. 17 (Fall 2009), http://www.securityaffairs.org/issues/2009/17/pongsudhirak.php.

16. Available at http://www.bangkokpost.com/tech/computer/39215/ministers-sign-computer-related-crime-mou.

17. Immediately after the coup, the coup makers made themselves known to the public as the Council for Democratic Reform under Constitutional Monarchy but usually used Council for Democratic Reform (CDR) as a shorter title. Later they changed the name to Council for National Security, or CNS.

18. The Computer-Related Offenses Act (also referred to as the cybercrime or computer crime act) was in the pipeline since 1992, involving several changes and draft versions.

19. "Thais to Sue Google over King Video" Al Jazeera, May 8, 2007, http://english.aljazeera.net/news/asia-pacific/2007/05/2008525131444839889.html.

20. For example, the Council of Europe's Cybercrime Convention, which is the main international standard in this field and provides a guideline for the development of national legislation as well as a framework for international cooperation, does not address content regulation but instead calls for self-regulation or coregulation in relation to Internet content. Council of Europe, Convention on Cyber Crime CETS No. 185, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

21. Translation of the Computer-Related Offenses Act, Vol. 124, Section 27 KOR., Royal Gazette, 18 June 2007, p. 7. Available at http://www.itac.co.th/index.php?option=com_content&view=article&id=90.

22. Sawatree Suksri, et al., *Situational Report on Control and Censorship of Online Media through the Use of Laws and the Imposition of Thai State Policies* (Bangkok: Heinrich Böll Foundation Southeast Asia, December 8, 2010), http://www.boell-southeastasia.org/downloads/ilaw_report_EN.pdf.

23. Sinfah Tunsarawuth and Toby Mendel, *Analysis of the Computer Crime Act of Thailand,* http://www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf.

24. Translation of the Computer-Related Offenses Act, Vol. 124, Section 27 KOR., Royal Gazette, 18 June 2007, p. 7. Available at http://www.itac.co.th/index.php?option=com_content&view=article&id=90.

25. "Web Censoring Needs a Debate," *Bangkok Post*, January 6, 2009, http://www.bangkokpost.com/opinion/opinion/9202/.

26. Translation of the Computer-Related Offenses Act, Vol. 124, Section 27 KOR., Royal Gazette, 18 June 2007, p. 7. Available at http://www.itac.co.th/index.php?option=com_content&view=article&id=90.

27. Interview with Chiranuch Premchaiporn and the author.

28. Somkiat Tangnamo passed away in July 2010.

29. Nida Moryadee, "OK Nation Blog as Citizen Journalism," unpublished master's thesis, Chulalongkorn University, 2009, 2–12.

30. See the Thailand country profile in this volume for further details.

31. Reporters Without Borders, "Government Uses State of Emergency to Escalate Censorship," April 8, 2010, http://en.rsf.org/thailand-government-uses-state-of-emergency-08-04-2010,36968.

32. Translation of Constitution of the Kingdom of Thailand B.E.2550 (2007). Available at http://www.isaanlawyers.com/constitution%20thailand%202007%20-%202550.pdf.

33. Translation of Thai Penal Code B.E. 2499 (1956), Section 112. Available at http://thailaws.com/law/t_laws/tlaw50001.pdf.

34. Standing during the royal anthem in a movie theater is a customary practice in Thailand to show respect and allegiance to the king.

35. "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.

36. "Aussie Author Gets Three-Year Sentence for Lèse-Majesté," *Bangkok Post*, January 20, 2009, http://www.bangkokpost.com/news/local/10026/aussie-author-gets-three-year-jail-sentence-for-lese-majeste.

37. "Lèse-Majesté Suspect Flees," *Bangkok Post*, February 10, 2009, http://www.bangkokpost.com/news/local/136371/lese-majeste-suspect-flees.

38. "Eighteen Years in Jail for Da Torpedo," *Bangkok Post,* August 28, 2009.

39. Based on data of the National Electronic and Computer Technology Center (NECTEC), Thailand has six international Internet gateways (IIGs): CAT Telecom Plc, TOT Plc, TRUE Corporation, Thai Telephone and Telecommunications (TT&T), ADC, and CS Loxinfo. These six IIGs also serve as National Internet Exchange (NIX). Of these six IIGs, two—CAT Telecom Plc and TOT Plc—are former state enterprises and monopoly telecommunications companies that have been corporatized, while two others—TRUE and TT&T—are long-time telecommunications concessionaires. Only ADC and CS Loxinfo are new market entrants and fully private entities. NECTEC's data also show that only 20 ISPs are actually carrying regular Internet traffic despite the fact that more than 40 ISPs hold licenses to operate.

40. Of the 20 operating ISPs, half are semiconcessionaires, as 35 percent of their shares are by default held by CAT Telecom, the long-standing international carrier monopoly. Although CAT Telecom's shares are wholly controlled by the Ministry of Finance, the corporatized state enterprise is under the bureaucratic structure of another government agency—MICT. This bureaucratic structure also helps explain the line of control in monitoring and filtering Web sites in Thailand. A number of ISPs are not under this bureaucratic structure, however. These are new operators that emerged as a result of a telecommunications reform process that has been ongoing since

the 2004 establishment of the National Telecommunications Commission (NTC), the country's first independent regulator of telecommunications. NTC has been issuing licenses for telecommunications services and Internet services since 2005. So far, a total of 130 licenses have been issued for telecommunications service and 132 for Internet. This description, therefore, reflects a two-tiered structure of Internet regulation. On one side, there are the pre-reform semiconcessionaires who are highly liable to CAT Telecom, which answers directly to MICT. On another side, there are the postreform ISPs that operate under licenses issued by NTC. This structure leads to somewhat of a double standard in Internet regulation and filtering.

41. URL filtering is one of the Web-content-filtering techniques. Content filters act on either the content or the information contained in the network packet header or body. URL filtering focuses on the URL and is suitable for blocking a Web page or sections of Web sites. There are two common approaches for URL filtering—pass-through filtering and pass-by filtering. Unlike pass-through filtering in which network traffic (a stream of packets) must pass through the filtering engine (firewall, proxy, or application gateway) for content inspection and can cause extra delay, pass-by filtering network packets do not have to "go through" the filtering engine. The filtering engine normally connects to a mirror port of a switch/gateway and passively monitors packets that pass through the switch (hence the term *pass-by*). Pass-by filtering is more flexible and therefore chosen for the Thai URL filtering system.

42. Robert Faris and Nart Villeneuve, "Measuring Global Internet Filtering," in *Access Denied: The Practice and Policy of Global Internet Filtering*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2008), 87.

43. Lawrence Lessig describes "traceability regulation" as a requirement by the state for service providers to employ software that facilitates traceability by making access conditional on the users' providing some minimal level of identification. Lessig, *Codes and Other Laws of Cyberspace*.

44. Warapong Theprongthong, "Content Regulation of Political Online Discussion Forums, after the Enforcement of the Computer-Related Offenses Act 2007," unpublished master's thesis, Chulalongkorn University, 2010, 54.

45. Ethan Zuckerman, "Intermediary Censorship," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (Cambridge, MA: MIT Press, 2010), 71–85.

46. Thai Netizen Network (TNN) is an interest group of Internet users who gathered to advocate on five basic principles—right to access information, freedom of expression, right to privacy, self-regulation, and creative commons—for online media. The group was founded in 2008 and comprises mainly people of the Net generation from various occupational backgrounds. See Thai Netizen Network, http://thainetizen.org.

47. Campaign for Popular Media Reform (CPMR), formerly the Committee to Monitor the Implementation of Article 40, was founded in 1997 by networks of academics, nongovernment organizations, mass-media practitioners, and civic media groups. These founders have played an active role in campaigning and participating in the course of Thai media reform since 1992.

CPMR's objective is to democratize communication in Thailand by promoting the transparency of media structure and the creation of a public sphere for communication. See Campaign for Popular Media Reform, "About Us," http://www.media4democracy.com/eng/about_us.html.

48. Freedom against Censorship Thailand (FACT) describes itself on its Web site as "a network of people who disagree with state censorship. We are a member organization in the Global Internet Liberty Campaign (GILC) and the Global Internet Freedom Consortium and cooperate with 200+ organisations around the world." See Freedom against Censorship Thailand, "About," http://facthai.wordpress.com/about.

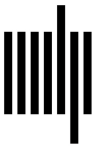
Access Contested

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