Volume 2 No. 6, June 2012 ISSN 2223-4985

International Journal of Information and Communication Technology Research

http://www.esjournals.org

The Analysis of the Computer Crime Act in Thailand

Danuvasin Charoen
NIDA Business School
National Institute of Development Administration
Bangkok, Thailand

ABSTRACT

The Computer Crime Act has been enforced in Thailand for five years. However, it has already created a great deal of concern and controversy from both inside and outside the country. The Computer Crime Act has been an important legal tool for the Thai Government to shut down or block thousands of websites and to prosecute a large number of individuals. Especially, the act has been criticized as a violation of freedom of expression on the Internet, which can greatly impact the growth of the Internet market in Thailand. The purpose of this study is to explore some of the controversial issues surrounding the Computer Crime Act in Thailand. The paper contends that the Computer Crime Act is an overly punitive and largely ineffective approach to combating computer/Internet crime. This is a descriptive research, and the data collection involves document analysis. The data were collected from secondary sources, such as research databases, news, and reports. The Thai government can use the results of this study to amend the law, and the results of the study can also be used to guide any nation to formulate or revise its computer crime laws.

Keywords: *Computer Crime Act, Computer Crimes, Computer Security, Freedom of Expression on Internet*

1. INTRODUCTION

The information and communication technology (ICT) business is comprised of four main segments: computer hardware, computer software, computer services, and telecommunication (wired and wireless). Driven by the increasing use of technology in all aspects of society, the industry had been growing rapidly in Thailand as in other countries around the globe, as an ever-expanding diversity of products, lower prices, and wider access to knowledge about how to utilize the various technologies has bolstered demand in the public, private, and civil society sectors. In consequence, by 2010, the Thai ICT market, accounting for 11% of the GDP, had risen to become one of the largest in the Southeast Asian region and was projected to grow at a compound annual growth rate of 12% over the 2010-2014 period [1]. The total value of Thai domestic spending on IT products and services, which had been in the vicinity of US$5.4bn in 2010, was expected to reach US$8.7bn by 2014 [1].

Increased usage of the Internet and software applications [2] has steadily pushed upward the overall market value of the industry. Total ICT market value increased every year from 2009 to 2011, when it reached a value of $22,621 million, with a solid 11.7% growth from the previous year. By far the largest contributor to the market value was the telecommunications industry, which accounted for 61.7% (or $13,945 million) of the total ICT market. The remaining segments, in declining order of the magnitude of contributions to the overall market value, were computer hardware shares (at 14.8%, for a market value of $3,350 million), software shares (at 12.4%, for a market worth of $2,807 million), and services (at 11.1% shares, for a market value of $2,519 million [1-2].

Underlying the above-cited market values and growth rates of the several industry segments lay distinct behaviors concerning the use of ICT technology. For example, on the institutional side, while every business trade and service has been able to increase its efficiency in lowering production costs and creating new markets for products and services, the hospital business in Thailand was the one in which the proportion of employees using computers and the Internet at work was the highest (100% and 90%, respectively). The next highest was manufacturing, travel agencies, construction, and business trade and services, respectively.

However, SMEs have been slow to adopt ICT, despite the fact that research has indicated the positive effect of ICT on firm performance in terms of creating productivity, profitability, market value, and market share. Further, the size of the particular establishment impacted the usage of ICT. Establishments with fewer than 16 persons used ICT to a slight degree: computer usage - 21.9%; Internet usage - 14.2%; and websites - 6.2%. By contrast, establishments with 16 persons or more used ICT at a high proportion, e.g., with more than 81.1% of establishments using computers [3]. Among educational institutions, 99.7% of primary educational institutions had computers, while other levels of educational institutions had computers in every institution. Further, the overwhelming major of educational institutions had Internet access. For instance, Internet access for primary educational institutions, at the vocational and non-formal education levels, and the higher education institutions, was 97.2%, 99.0%, and 100.0%, respectively.

At the level of the individual person and individual households, mobile phone popularity had rapidly increased from 28.2% in 2004 to 56.8% in 2009. However, the proportion of the population using computers and the Internet increased less robustly, going from 21.4% to 29.3% for computers during the 2004-2009 period, and from 11.9% to 20.1% for the Internet. Moreover, the Internet access of households increased very modestly, from 5.7% in 2004 to 9.5% in 2009; and, broadband Internet access increased from

Volume 2 No. 6, June 2012 ISSN 2223-4985

International Journal of Information and Communication Technology Research

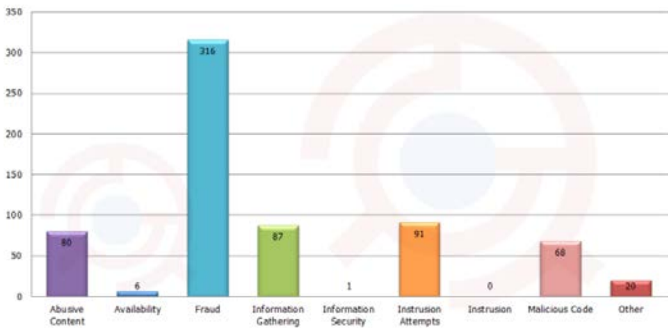
http://www.esjournals.org

52.8% in 2006 to 55.1, while fixed-line telephones decreased from 23.4% in 2004 to 21.4% in 2009 [3]. In 2011, Thailand was ranked 9th in Asia in terms of Internet users [4] .

In 2011, Thailand was ranked 38th (out of 134 countries) in the global competitiveness report conducted by the World Economic Forum. It also was ranked well below the world average on all of the factors related to technology, despite the fact that information technology and telecommunications had been a major factor driving the competitiveness of the country. More specifically, the major problems for Thailand were concerned with the "pillar of technological readiness" – a measure used by the World Economic Forum to assess a nation's capacity to utilize information and communication technologies. Thailand was ranked 86th in number of Internet users, 64th in availability of the latest technologies, 66th in firm-level technological absorption, 88th in broadband Internet subscriptions, and 75th in Internet bandwidth [5].

Over the past twenty years, the Internet has transformed many aspects of modern life in Thailand. People can communicate and collaborate faster and better due to the Internet, and the Internet has become a necessary tool for both business and for leisure. As of June 2011, there are 18 million people (accounting for 27% of the population) accessing the Internet [4]. However, one of the fastest-growing crimes in Thailand is the crime related to the use of computers and the Internet [6], and these crimes can have a negative impact on both businesses and individuals.

Cyber Crime Statistics in 2011 [7]



In 2011, the total number of computer crimes reported was 660. Fraud was the highest computer crime reported. The second and the third were information gathering and abusive content. The total number of reported computer crimes in 2011 was 660 cases [7].

Crime Statistics in 2011 [7]

Types	Total
Abusive content	80
Availability	6
Fraud	316
Information gathering	88
Information security	0
Intrusion Attempts	91
Intrusion	0
Malicious code	68
Other	11
Total	660

2. COMPUTER CRIME ACT

It has been five years since the enactment of Thailand's controversial Computer Crime Act, a law that several experts indicate hinders free expression on the Internet. This law was introduced in 2007 under the post-coup government led by General Surayudh Chulanont and it came into force when the Internet had already become prevalent among Thai people. The Internet allows information among individuals and businesses, especially social media and social networks, and also provides a means for people to express their opinion and share information with others in the network. Many Thai Internet users use web boards, blogs, and social networks to share their views on social, economic, and political issues. The Internet provides the means for them to express their opinion without being screened or censored. Users can remain anonymous. Social networks such as Facebook, Hi5, Myspace, LinkInn, and Twitter have become increasingly popular among Internet users in Thailand.

The Computer Crime Act has been criticized for its unclear provisions and harsh penalties. For example, the law empowers authorities to block or shut down websites considered harmful by the State [8]. The crimes that this law addresses range from spreading viruses to posting inappropriate contents such as those considered harmful to national security or *lèse majesté*. The penalty also has been broadened to include the ISP and website administrators that host inappropriate content (Section 15). In addition, section 14(4) indicates the penalty for anyone that helps disseminate inappropriate content. The act of dissemination includes email forwarding, retweeting a twitter, or sharing content on Facebook.

Before the enactment of the Computer Crime Act, Thai authorities did not have any specific legal tool with which to address issues such as hacking, disclosure of access passwords to a third party, eavesdropping on computer data, pornography and other "harmful" Internet content, or the liability of ISPs. Some of these offences could be prosecuted under Thailand's Penal Code or Criminal Code, but the Computer Crime Act establishes more specific charges and, in some cases, heavier penalties. Importantly, the Act also gives competent officials the power to restrict the dissemination of computer data or websites.

3. LITERATURE REVIEW

National Response to Cyber Crime

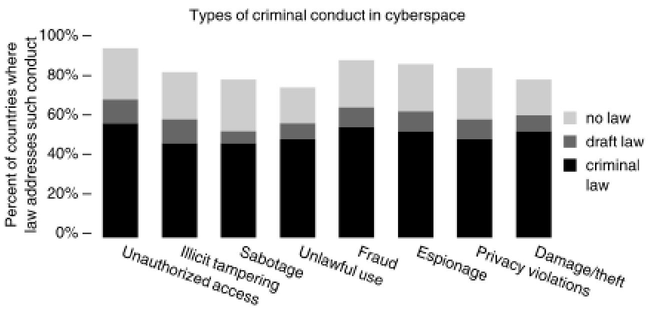
Several nations have recognized that computer and Internet crime can seriously threaten infrastructure, commercial interests, and public policies. As a result, several

Volume 2 No. 6, June 2012 ISSN 2223-4985

International Journal of Information and Communication Technology Research

http://www.esjournals.org

countries have developed legal codes to combat computer-related crimes [9]. Most countries having laws against computer and Internet crimes usually include some or most of the following acts: 1, unauthorized access; 2, illicit tempering with files or data (such as unauthorized copying, modification, or destruction; 3, computer or network sabotage (viruses, worms, Trojan horses, and denial of service attacks; 4, use of information systems to commit or advance “traditional” crimes (such as fraud, forgery, money laundering, acts of terrorism; 5, computer-mediated espionage; 6, violations against privacy in the acquisition or use of personal data; and 7, theft or damage of computer hardware or software [9].



Source: Putnam, T. L., & Elliott, D. D. (2001). International Responses to Cyber Crime. In S. E. Goodman & A. D. Sofaer (Eds.), The Transnational Dimension of Cyber Crime and Terrorism: The Hoover Institution Press.

National response to Computer and Internet-related crimes [9]. The above figure indicates the differences in cyber crime acts among countries [9].

	Theft of electronic data	Destruction or damage of a computer system	Disclosure of secrets	Computer fraud	Unauthorized access	Forgery of e-document	Defamation/libel	Business disparagement	Obscenity
Taiwan	•	•	•	•	•	•	•	•	•
Hong Kong	•	•	•	•	•	•	•	•	•
China	•	•	•	•	?	•	•	•	•
Japan	•	•	•	•	•	•	X	X	X
Singapore	•	•	□	•	•	•	•	•	•
Thailand	•	•	•	•	•	•	•	•	•
Vietnam	X	X	X	X	X	X	•	•	•
Malaysia	•	•	•	•	•	•	X	X	X

•=prohibited □=weakly or incompletely prohibited X=no prohibition ?=unknown

Source: Putnam, T. L., & Elliott, D. D. (2001). International Responses to Cyber Crime. In S. E. Goodman & A. D. Sofaer (Eds.), The Transnational Dimension of Cyber Crime and Terrorism: The Hoover Institution Press.

International Response to Cyber Crime

The above figure indicates categories of computer and network misuse that are considered as the crimes in Asia [9]. These include the following actions: theft of electronic data; destruction or damage of a computer system; disclosure of secrets; computer fraud; unauthorized access; forgery of e-documents; defamation; and business disparagement and obscenity [9]. Each country also has different interpretations of criminal computer acts. For example, the Taiwanese computer crime acts make it an offense to commit fraud by means of the “input false information or commands into a computer or related device, to infringe on copyright, or to appropriate the possessions of others.” Other countries’ acts include “libel,” “business disparagement,” “obscenity,” “making threats,” “gambling on the Internet,” and “disclosure of secrets” [9]. In Japan and Thailand, unauthorized access to a computer in which people may view secret information is illegal even if there is no damage done to the systems. In Singapore, “unauthorized access”, “disclosure of secrets”, “destruction or damage of computer systems or electronic data”, and “computer fraud” are illegal. In Malaysia, the illegal acts include defamation and libel, business disparagement, and obscenity offenses. In Hong Kong, the illegal acts include “defamation”, “business disparagement”, “offenses against e-mail”, “damage and destruction”, “computer fraud”, and “theft of electronic data”. In China, computer crimes are included in Articles 285-287 of the Criminal Code. The offenses include “illegally transferring in the operation of a computer system,” which is punishable by a minimum sentence of five years in prison [9].

Internet Censorship

Censorship has been a controversial issue on the Internet. Internet censorship can be defined as the control or suppression of publishing or accessing information on the Internet. Usually, Internet censorship is carried out by governments or by private companies on behalf of the government or on their own initiative [10].

Computer Crime Act and Related Law

Before the enactment of the Computer crime Act, Thai authorities did not have any specific legal tool with which to address issues such as hacking, disclosure of access passwords to a third party, eavesdropping on computer data, pornography and other “harmful” Internet content, or the liability of ISPs. Some of these offences could be prosecuted under Thailand’s Penal Code or The Criminal Code, but the Computer Crime Act establishes more specific charges and, in some cases, heavier penalties. Importantly, the Act also gives the competent official the power to restrict the dissemination of computer data or websites.

Criminal Trends

Thailand has launched the ICT plan (framework 2010) by delivering the advantage of ICT technology as a strategy to develop the country to be a “**Wisdom and**

International Journal of Information and Communication Technology Research

http://www.esjournals.org

Learning Society;" namely, E-industry, E-commerce, E-government, E-education, and E-society. The introduction of ICT is accompanied by new serious threats and dangers by cyber criminals. Cyber crime is on-going and growing in Thailand.

Technology Crime Case 2010-2011 (Jan-Oct)

Nature of Case	2010	2011 (Jan – Oct)
1. System-Related Offences (Illegal access/attacking a system/damaging, destroying, changing the data in computer systems)	16	13
2. Defamation/Les Majesty	3	6
3. Internet Fraud/Cheating	11	8
4. Internet Gambling	15	14
5. Content-Related Offences (Import forged/false data/Pornographic /computer data against Kingdom security)	21	387
6. Others (Extortion, Illegal Drugs)	7	3
Total	73	431

Source: Apichanont, A. (2011). *Country Report*. Bangkok, Thailand: Technology Crime Suppression Division.

According to the Technology Crime Suppression Division of Thailand, the statistics on computer crime offences totalled 73 cases in 2010. In the next year, 2011, the number of crimes rose extremely, to 431 cases [11]. The top computer crimes include attacks against computer data and systems, Les Majesty, Identity Theft, Defamation, Importing a forged or false computer system, Internet Gambling, and Internet Fraud [11].

4. RESEARCH METHOD

This is a descriptive research. The data collection involves document analysis, and the data were collected from secondary sources, such as research databases, news, and reports related to the Computer Crime Act.

Overview of Computer Crime Act

The Computer Crime Act came into force on 18th July 2007 under Prime Minister Surayud Chulanont. It is one of the first bills passed by the National Legislative Assembly installed by the military after the September 2006 coup that toppled former Prime Minister Thaksin Shinawatra. Before 2007, Thai authorities did not have any legal tools with which to tackle issues such as hacking, stealing of digital information, eavesdropping on computer data, disclosure of passwords to unauthorized parties, and posting pornography and other inappropriate content on the Internet. Some of these offenses can be prosecuted under Thailand's Penal Code. However, the Computer Crime Act provides more specific charges and in many cases, heavier penalty [12]. Especially, the Computer Crime Act also provides power to authorities to block or shut down any websites they considered unlawful [12].

The Computer Crime Act has two parts. The first part (Section 8 to 17) covers computer-related offences, and the second part (Section 18 to 30) covers the roles of authorities and the responsibilities of service providers. The offences in the Computer Crime Act include the following:

Unauthorized Access to a Computer System

Sections 5 and 6 deal with unauthorized access to computer systems. Section 5 provides for imprisonment up to six months and/or a fine of up to 10,000 baht (approximately US$300) for unauthorized accessing a computer system. Section 6 provides for double the maximum jail term and the maximum fine for disclosing an access code for a computer system in a manner that is likely to cause damage to other people.

Unauthorized Access to Computer Data

Sections 7 and 8 deal with unauthorized access to computer data. Section 7 provides for imprisonment up to two years and/or a fine of up to 40,000 baht (approximately US$12,000) for unauthorized accessing computer data. Section 8 increases the penalty to a maximum imprisonment of three years and/or a maximum fine of 60,000 baht (approximately US$1,800) for illegally eavesdropping by electronic means on computer data not intended for use by the general public.

Illegally Damage Computer Data or Computer Systems

Sections 9 and 10 punish those who illegally damage computer data or computer systems. Section 9 provides for imprisonment of up to five years and/or fine of 100,000 baht (approximately US$3,000) for illegally damaging, destroying, amending, alerting or adding to a third party's computer data. Section 10 provides for the same penalty for illegally suspending, delaying, hindering or disrupting the working of a third party's computer system to the extent that it fails to function as usual.

Spam

Section 11 deals with spam. Spam in this act includes sending computer data or emails to another person by concealing or forging the source of the data or email in manner that interferes with the use of that computer system by other people. The section provides for a fine of up to 100,000 baht (approximately US$3,000), but not for imprisonment.

Causing Damage to Public or National Security

Section 12 provides for heavier potential penalties for causing damage to the public or a large number of people. The section provides imprisonment up to 10 years and a fine up to 200,000 baht (approximately US$6,000) for section 9 and 10 offenses where they cause instant or subsequent damage to the public. The penalty can be raised to imprisonment of up to 15 years and a fine of up to 300,000 baht (approximately US$9,000) where the offences are likely to cause damage to computer data or computer systems related to public and national security, economic security, and public service and infrastructure. The maximum imprisonment can be raised to 20 years if the offences cause death.

The distributors of computer programs for the purpose of committing an offence under Sections 5 to 11

Section 13 provides for imprisonment of up to one year and/or a fine of up to 20,000 baht (approximately US$600) for those selling or disseminating any computer program or set of instructions in order to commit crimes under Section 5 to 11.

Importing Illegal Data into a Computer System

Section 14 provides for imprisonment of up to five years and/or a fine of up to 100,000 baht (approximately US$3,000) for a variety of offences, including importing false data into a computer system is are likely to cause damage to a third party or the public (sub-section 1), false data in a manner that can cause public panic (sub-section 2), data constituting an offence against national security (and royal family) under the Penal Code (sub-section 3), pornographic data (sub-section 4), or disseminating these contents.

The Role of Internet Service Providers (ISPs)

Section 15 allows authorities to charge any ISPs that intentionally supports or gives consent to the commission of an offence under Section 14. The term “intentionally” protects ISPs that are not aware of the contents on their systems. Nevertheless, after the ISPs are informed about the illegal content, this defense no longer applies. If any ISP is found guilty, he or she can face a penalty equal to that imposed on the offender.

Defamation

Section 16 deals with defamation by visual means. Section 16 provides for imprisonment up to three years and/or a fine of up to 60,000 baht (approximately US$ 1,800). This section punishes those that make publicly accessible via a computer system a picture of a third party in a manner that is likely to damage that third party’s reputation or to cause that third party to be disgusted or embarrassed.

Controversial issues surrounding the Computer Crime Act

Lese Majeste

In Thailand, the head of the state is the king. The power of the king is limited to being a symbolic figurehead, but the institution demands respect and reverence from the people [13]. Lese majeste has been the single offence most frequently applied by the Thai authorities against Internet users and ISPs under the Computer Crime Act due to the recent political situation. The lese majeste crime has become a matter of domestic and international concern as issues related to politics since the military coup in 2006. For example, in 2011, a Thai-born American named Joe Gordon was arrested for translating part of a banned biography of King Bhumibol Adulyadej and posting it on the Internet. He was arrested during his visit to Thailand for medical treatment. Mr. Gordon said "I am an American citizen, and what happened was in America." However, the official argued that the Computer Crime Act applies to anyone, including foreigners committing the offence outside the country [14]. Thailand has been criticized worldwide for its lese majeste laws in recent years. People that commit Lese Majeste can be sentenced between three and five years. The Computer Crime Act enables prosecutors to seek longer sentences if the offenders are found guilty of using the computer and Internet to commit a crime. The U.S. consul general in Thailand, Elizabeth Pratt, mentioned that “Washington considered Mr. Gordon's sentence severe because it had been imposed for his exercising his right to freedom of expression" [14]. Lese Majeste continues to be the most controversial issue related to the Computer Crime Act.

Another case is that of Mr. Suwicha Thakhor. On YouTube, he was known as “thaiman 8,” a prolific poster of rude videos that ridiculed Thailand’s royal family. In January 2009, Mr. Suwicha Thakhor was arrested while shopping with his wife in Nakhon Phanom. In April 2009, he was sentenced for ten years in jail after pleading guilty to lese majeste, the crime of defaming or threatening the Thai crown and for posting defamatory materials about King Bhumibol Adulyadej on YouTube [11, 15] .

Moreover, in mid-October 2009, Thai stock prices fell for two consecutive days, following rumors posted on the Internet that King Bhumibol’s health had deteriorated after he was hospitalized in mid-September. The King has since made several public appearances on various occasions. As of late April 2011, he remains in the hospital.

Volume 2 No. 6, June 2012 ISSN 2223-4985
International Journal of Information and Communication Technology Research

http://www.esjournals.org

In November 2009, Thai authorities arrested four people that were staff members at KT-Sefigo, Ltd., and chief executive officer of The UBS securities (Thailand) Ltd., under Section 14 of the Computer Crime Act for posting the false data into a computer system which was likely to damage national security or to cause a public panic [11].

Pornographic Data

Pornography on the Internet has been controversial in many countries. However, the line between the pornographic and artistic is often blurred. In many countries, the law prohibits sexual materials only for minors.

Internet Service Providers

Section 15 allows authorities to charge any ISP or service provider that intentionally supports or consents to the commission of an offense under Section 14. The service providers include website and webboard owners that host material prohibited by Section 14. Several critics have argues that ISPs and service providers should not be subject to the same penalty as the primary offenders because they only provide technical service and do not create the (illegal) content.

One of the recent cases according to this section is that of Ms. Chiranuch Permchaiporn, who is the web master of Thailand's popular Prachathai news website. She was charged under section 15. Her crime was to fail to remove quickly enough comments posted by an anonymous user. According to the Financial Times, Ms. Permchaiporn argued that

"It has created a climate of fear. I didn't say anything, I didn't write anything, I didn't post anything but as webmaster [editor] I am facing the penalty" [16].

The Chiranuch case has potential implications for Internet giants such as Google and Facebook.

"If they [Internet access providers] are found to be liable, it would be very detrimental to the whole digital economy of Thailand," says John Ure, the executive director of the Asia Internet Coalition, a pressure group set up by Google, Ebay, Skype and others. "E-commerce, social networking and the like would all be completely disrupted" [16].

Defamation

Section 16 makes it a crime for making publicly accessible via a computer system a picture of a third party in a manner that is likely to "impair that third party's reputation or cause that third party to be embarrassed." Section 16 only deals with defamation by visual means. It does not cover defamation by means of written text, which is already covered by the defamation provisions in the Penal Code. However, the jail term of Section 16 is higher than that in the Penal Code, which has only a two-year sentence. This is contrasted with the crime of lese majeste, for which the penalties in the Penal Code are much higher. Several website operators and web administrators have been charged with defamation under the Computer Crime Act. It is interesting to note that in most countries images are not included in the definition of defamation because they are subjective in terms of interpretation. In most developed, democratic nations, defamation applies to defamatory statements on the Internet. In addition, criminal defamation can be viewed as a restriction on freedom of expression [12].

Too much power for the Authorities

The Computer Crime Act grants authorities vast power to investigate, gather, and confiscate evidence of any suspect committed computer crimes. Section 18 allows authorities to copy computer data and/or computer traffic data (log files) from any computer system suspected of being used to commit crimes. Under Section 18, the authorities also have legal power to access any computer system and/or computer data, and to seize or attach any computer systems for up to 90 days, for the purposes of investigation and gathering evidence. Section 20 allows authorities, with the approval of the Minister of Information and Communication Technology, to seek a court warrant limiting the dissemination of the information directly or asking an ISP to do so.

The Wall Street Journal reported that Thai authorities have blocked at least 40,000 web pages in 2010, according to the Ministry of Information and Communication Technology, which monitors the Internet in Thailand. However, free speech advocates have stated that authorities re actually blocking at least 110,000 sites based on government disclosures and their online checking [17]. Many of the blocked websites are related to the criticism of the government or attacks on Thailand's revered monarchy [17]. Free speech activists argue that the government has overstated the threats as a justification to block websites [17]. The most-cited example is www.prachathai.com, which positions itself as an independent news source that contains articles and reports questioning the policies of the government [17].

The Computer Crime Act incurs the Cost of doing Business

Section 26 indicates that service providers must store computer traffic data for at least ninety days from the date on which the data was input into computer systems. Nevertheless, if needed, authorities may order service providers to store computer traffic data for a period longer than ninety days but not more than one year. Under this section, the service provider must store the necessary information of the service to be able to identify the user of the service. Any service provider that fails to comply with this section will be fined up to 500,000 baht (approximately US$ 17,000). The definition of service providers can be categorized into 4 types:

1. Telecommunication and broadcast carriers include:

   1.1. Fixed line service providers
   1.2. Mobile service providers
   1.3. Leased circuit service providers included fiber optics, ADSL (Asymmetric Digital Subscriber Line), Frame Relay Providers, ATM (Asynchronous Transfer Mode) excluded Physical media providers or Cable (Dark Fiber providers that do not contain Internet or IP traffic)
   1.4. Satellite Service Providers

2. Access Service Providers include:

   2.1. Internet service providers (both wire or wireless)
   2.2. Operators that provide Internet access in offices/rooms, rental rooms, hotels or restaurants
   2.3. Computer network access service providers for organizations such as governmental departments, and companies or academic institutions

3. Hosting Service Providers include:

   3.1. Web hosting or rental web hosting
   3.2. File Servers or file sharing
   3.3. Mail Servicer Service Providers
   3.4. Internet Data Centers

4. Internet Cafés include:

   4.1. Internet Cafes
   4.2. Game Online

The purpose of this section is for the law enforcement to be able to gather evidence of the offence and to trace the identity of the offenders. In other words, this section attempts to prevent anonymous use of the Internet. The requirements of this section incurred the cost of doing business, especially for SMEs because organizations have to invest in the system (hardware and software) to keep computer traffic data (log files). The software alone can cost around 100,000 baht (approximately US$ 3,400). The whole system can range between one (approximately US$ 34,000) and ten million baht (approximately US$ 340,000) [18].

Contributions of the Study

This study presents several problems and issues in relation to The Computer Crime Act and its consequences in Thailand. The study contributes to the literature on the Computer Crime Act. The Thai government can use the results of this study to amend the law, and the results can also be used to guide any nation to formulate or revise their computer crime acts.

5. CONCLUSIONS

The Computer Crime Act has been in force for five years and has impacted a large number of businesses and individuals in Thailand. The Computer Crime Act has been criticized for its unclear provisions and harsh penalties. It also has been largely criticized regarding the violation of freedom of expression on the Internet from both inside and outside the country. This study presents several controversial issues related to the Computer Crime Act in Thailand. The results of this study can be used to guide the nation to amend the law. The study contributes to the literature on computer laws and enforcement.

REFERENCES

[1] NECTEC, Thailand ICT Market. 2009, Software Indusry Promotion Agency National Electronics and Computer Technology Center.

[2] NSTDA, Thailand ICT Market and Outlook. 2011, National Science and Technology Development Agency.

[3] Santipaporn, S. Information and Communication Technology Statistics in Thailand. in International Seminar on Information and Communication Technology Statistics. 2010. Seoul, Republic of Korea.

[4] internetworldstat.com. Asia Internet Usage and Population 2011 Jan 2]; Available from: http://www.internetworldstats.com/stats3.htm

[5] NECTEC, Thailand ICT Market. 2009, Software Indusry Promotion Agency National Electronics and Computer Technology Center.

[6] NSTDA, Thailand ICT Market and Outlook. 2011, National Science and Technology Development Agency.

[7] Santipaporn, S. Information and Communication Technology Statistics in Thailand. in International Seminar on Information and Communication Technology Statistics. 2010. Seoul, Republic of Korea.

[8] internetworldstat.com. Asia Internet Usage and Population 2011 Jan 2]; Available from: http://www.internetworldstats.com/stats3.htm

[9] Forum, W.E., The Global Competitiveness Report 2010-2011 2011.

International Journal of Information and Communication Technology Research

http://www.esjournals.org

[10] ThaiCert, Year 2007 ThaiCERT's handled Incident Response Summary, N. Sanglerdinlapachai, Editor. 2007, Thai Computer Emergency Response Team.

[11] ThaiCert, Cyber Crime Statistics in 2011. 2011, Thai CERT: Bankgkok.

[12] Singh, A., Thailand's Computer Crime Act still a major threat to free expression. 2010, Thailand Business News.

[13] Putnam, T.L. and D.D. Elliott, International Responses to Cyber Crime, in The Transnational Dimension of Cyber Crime and Terrorism, S.E. Goodman and A.D. Sofaer, Editors. 2001, The Hoover Institution Press.

[14] Wikipedia. Internet Censorship. 2012 [cited 2012 Jan13]; Available from: http://en.wikipedia.org/wiki/Internet_censorship

[15] Apichanont, A., Country Report. 2011, Technology Crime Suppression Division: Bangkok, Thailand.

[16] Tunsarawuth, S. and T. Mendal, Analysis of Computer Crime Act of Thailand. 2010.

[17] Wikipedia. Monarchy of Thailand. 2012 [cited 2012 Jan 3rd]; Available from: http://en.wikipedia.org/wiki/Monarchy_of_Thailand

[18] Hookway, J., U.S. Man's Jailing Spotlights Thai Monarch Law, in Wall Stree Journal. 2011: New York, N.Y.

[19] Annoymous, Asia: Treason in cyberspace; Thailand's lese majeste law, in The Economist. 2009.

[20] Johnson, T., Draconian Thai law lands editor in court over online posting, in Financial Times. 2011: London (UK).

[21] Barta, P., Thai Groups Denounce Website Censorship; Government Blocks Thousands of Pages Following Clashes, in Wall Street Journal 2010, Wall Street Journal: New York, N.Y. .

[22] Annoymous, Log Files and Computer Crime Act, in Thanonline.com. 2008: Bangkok.