KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS ON THAILAND'S PROPOSED COMPUTER-RELATED OFFENSES COMMISSION ACT

March 2012

Thailand's Computer Crime Act of 2007 has been criticized for being overbroad and for granting authorities too much discretion in prosecuting Thai citizens and online service providers. However, a Draft Bill to replace the CCA suffers from many of the same defects. Vague, overbroad, or overly punitive provisions in the Draft Bill could inhibit Thai service providers from offering Web 2.0 services and could harm Thailand's global economic competitiveness in the Information Age. Rather than establishing new offenses and additional penalties for crimes committed with a computer, the Draft Bill should be revised to focus on crimes against computer systems, with precise and narrow definitions and generally limited to conduct intended to create harm.

I. Introduction

The Center for Democracy & Technology ("CDT") is honored to provide these comments on Thailand's proposed Computer-Related Offences Commission Act (2011) ("Draft Bill" or "Bill").[1]

CDT commends the Government of Thailand for undertaking to replace the 2007 Computer Crime Act of Thailand ("CCA") with a new cybercrime law. Thai and international experts have criticized the current CCA for being ambiguous and overbroad.[2] Reforming the CCA represents an opportunity to correct defects in the current law and harmonize Thai cybercrime law with international standards.

However, our review of the Draft Bill reveals that many of the problems with the CCA remain unaddressed by the Draft Bill. Much of the language in the Bill is vague or overbroad. A number of the provisions risk criminalizing ordinary and innocent conduct of computer users and service providers. Moreover, the Draft Bill fails to bring Thai cybercrime law into accord with international standards such as those set forth in the Council of Europe's Convention on Cybercrime ("COE Convention" or "Convention").[3]

Computer crime provisions, like any criminal law, should be sufficiently definite to make it clear to individuals what is prohibited and to prevent arbitrary or

---

[1] These comments are based on the English translation of the Draft Bill provided to CDT in December 2011. A copy of that English translation is attached to these comments as an appendix.

[2] *See* Sinfah Tunsarawuth and Toby Mendel, "Analysis of Computer Crime Act of Thailand," Center for Law and Democracy (May 2010), *available at* http://www.law-democracy.org/wp-content/uploads /2010/07/10.05.Thai_.Computer-Act-Analysis.pdf.

[3] Council of Europe, Convention on Cybercrime, ETC No. 185 (Nov. 23, 2001), *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

discriminatory enforcement. Vague laws give government officials too much discretion to decide which individuals to prosecute. Such laws are not only anti-democratic, but they also have a chilling effect on entrepreneurship and innovation. The vague, overbroad, or overly punitive provisions in the Draft Bill could inhibit Thai service providers from offering Web 2.0 services and could harm Thailand's global economic competitiveness in information and communications technologies ("ICTs").

CDT recommends specific changes to the Draft Bill.

II. Guiding Principles

A. The Principle of Technology Neutrality

Like the current CCA, the Draft Bill would establish special penalties for committing *with* a computer or *by* electronic means offenses that are already a crime under the Penal Code. Specifically, Section 23 would make it a crime to import into a computer system any data that is an offense relating to the security of the Kingdom or an offense relating to terrorism, matters already covered the Penal Code. Similarly, Section 27 would make it a crime to import into a computer system any information likely to cause damage to another person, impair his or her reputation, or expose him or her to hatred, contempt or embarrassment; some or all of those matters are already covered, we assume, under Thailand's laws concerning defamation and harassment.

As a general principle, there is no need for special penalties for crimes committed *with*, or facilitated *by*, the use of a computer. It is already a crime to commit larceny, for example. There is no need for a separate criminal provision making it a crime to commit larceny "by electronic means." This is the principle of technology neutrality.

Prevailing international standards recognize the principle of technology neutrality.[4] The Council of Europe's *Declaration on freedom of communication on the Internet* (2003) ("COE Declaration"), for example, states as its first principle:

> Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery.[5]

[4] *See* Council of Europe, Committee of Experts on Crime in Cyber-Space, Explanatory Report to the Convention on Cybercrime, ETS No. 185, ¶ 36, (May 25, 2001), *available at* http://conventions.coe.int/treaty/en/reports/html/185.htm (stating that the Convention "uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies").

[5] Council of Europe, Declaration on freedom of communication on the Internet, adopted May 28, 2003, *available at* http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2003)007_en.pdf. The COE Convention itself does not fully follow this principle, for it includes not only crimes against a computer or computer data but also certain offenses (child pornography offenses and copyright infringement) facilitated by a computer. COE Convention, Articles 7-10. However, the Explanatory Report makes it clear that States need only fill gaps in their law, not separately criminalize all illegal conduct where committed by electronic means:

This principle reflects the Council of Europe's determination that the use of a computer or the Internet to distribute unlawful content, in and of itself, does not typically justify enhanced criminal penalties. Content that is illegal when distributed by traditional, offline means is no less and no more illegal when distributed via a computer online. Similarly, conduct that is criminal remains criminal whether or not the conduct is committed "by electronic means."

Cybercrime is properly concerned with crimes committed *against* a computer or computer data, where traditional criminal provisions such as trespass and destruction of property may not be applicable due to the intangible nature of the activity or the harm.

This point is well illustrated with respect to the law of lese majeste. Of the 185 reported cases involving the CCA from July 2007 through July 2010, 31 were for lese majeste offenses.[6] In most instances, these cases were brought under both the CCA and the relevant lese majeste provisions of the Penal Code.[7] As international UN mechanisms have recommended, the nation may wish to re-evaluate the desirability of its lese majeste law in the future.[8] Regardless, even before that happens, there is no need for two laws punishing the same content. Accordingly, pursuant to the principle of technology neutrality, CDT recommends that Section 23 of the Draft Bill be stricken because the offenses are already contained in the Penal Code.

For the same reasons, CDT recommends that Section 27 be deleted. The Bill should focus on conduct committed *against* computers or computer data.

B. The Principle of Intentionality

Defining cybercrime offenses without regard to criminal intent can have unintended consequences, including punishing ordinary and innocent conduct of computer users. Under the COE Convention, all computer-related offenses must be committed intentionally.[9] For example, Article 2 of the Convention states:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed

---

Most States already have criminalised these ordinary crimes, and their existing laws may or may not be sufficiently broad to extend to situations involving computer networks (for example, existing child pornography laws of some States may not extend to electronic images). Therefore, in the course of implementing these articles, States must examine their existing laws to determine whether they apply to situations in which computer systems or networks are involved. If existing offences already cover such conduct, there is no requirement to amend existing offences or enact new ones. COE Explanatory Report, note 4 above, ¶ 79.

[6] Heinrich Böll Foundation, "Situational Report on the Control and Censorship of Online Media, through the Use of Laws and the Imposition of Thai State Policies" at p. 10 (Dec. 9, 2010), *available at* http://www.boell-southeastasia.org/downloads/ilaw_report_EN.pdf.

[7] Heinrich Böll report, note 6 above, at pp. 12-13. Section 112 of the Penal Code provides greater penalties for lese majeste offenses than the CCA and so authorities typically proceed under the Penal Code.

[8] *See* "UN expert recommends amendment of lese majeste laws" (October 10, 2011), http://ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=11478&LangID=E. In CDT's view, lese majeste laws violate the human right to freedom of expression, as expressed in international human rights instruments, including the *International Covenant on Civil and Political Rights* ("ICCPR"), to which Thailand is a signatory.

[9] *See* COE Explanatory Report, note 4 above, ¶ 39.

> intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

The CCA has been criticized for lacking intentionality requirements in a number of its provisions.[10] Unfortunately, the Draft Bill fails to introduce adequate intentionality requirements into Thai cybercrime law.

For example, Section 15 of the Draft Bill states that "Whoever wrongfully accesses a computer system or computer data of another person shall be punished with imprisonment not exceeding one year or a fine not exceeding twenty thousand baht, or both." The word "wrongfully," which is used throughout the bill, is not defined. Even if "wrongfully" were adequately defined in the Draft Bill, Section 15 is overbroad because it does not require that offenders specifically intend to "wrongfully" access the computer system or computer data of another person. Individuals who use the Internet access the data and computer systems of others as a matter of course and sometimes this access may be unknowingly in violation of terms of service or without the permission of the owner of the data or computer system.[11] As written, Section 15 gives government officials unfettered discretion to determine the types of access that are "wrongful" and then punish computer users for this access regardless of whether the individual actually intended to "wrongfully" access the data or computer system of another. Evenhanded administration of such a standard is not possible. This failure to include the principle of intentionality is a problem throughout the Draft Bill.

CDT recommends that the Draft Bill should be revised to include the principle of intentionality. This can be accomplished by inserting language such as, "knowingly," "willfully," "intentionally," or "with intent" to each substantive provision of the Bill.

C. Limits on the Criminal Liability of ICT Intermediaries for Third Party Conduct

ICT intermediaries are the Internet Service Providers ("ISPs"), hosting services, web forums, social networks, or search engines that make possible the storage, transmission and retrieval of communications and content by Internet users. It is widely recognized that these technical intermediaries should not be criminally responsible when they unknowingly distribute or host unlawful content created or uploaded by third party users. Many countries set limits on the criminal liability of ICT intermediaries for the illegal conduct of users.[12]

---

[10] *See* ARTICLE 19, *A Memorandum on the draft Computer-Related Offences Commission Act currently being developed by the Thai authorities* (April 2007), *available at* http://www.article19.org/data/files/pdfs /analysis/thai-internet-mar-07.pdf.

[11] *See* COE Convention Explanatory Report, note 4 above, ¶ 38 (noting that "legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized.")

[12] *See* Tunsarawuth and Mendel, note 2 above, at pp. 5-6. *See also* Asia Internet Coalition's statement on the Computer Crimes Act of Thailand (Sept. 8, 2011) ("AIC Statement"), *available at* http://www.asiainternetcoalition.org /advdoc/8887df8fd914ff2b80829a6a6327e91c.pdf; Center for Democracy & Technology, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation" at 7 (April 2010), *available at* http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf.

In the European Union, Articles 12 - 14 of the European Union's e-Commerce Directive (2000) grant immunity to ICT intermediaries that transmit or host illegal material uploaded by third parties, so long as the intermediary (1) does not have actual knowledge of the illegal material, and (2) quickly removes the material upon receiving such knowledge.[13]

Senior experts at the United Nations, the Organization for Security and Cooperation in Europe ("OSCE"), and the Organization of American States ("OAS") strongly supported protection of intermediaries from liability in a 2005 statement:

> No one should be liable for content on the Internet of which they are not the author, unless they have either adopted that content as their own or refused to obey a court order to remove that content.[14]

Similarly, Principle 6 of the 2003 COE Declaration states:

> Member states should ensure that service providers are not held liable for content on the Internet when their function is limited, as defined by national law, to transmitting information or providing access to the Internet.
>
> In cases where the functions of service providers are wider and they store content emanating from other parties, member states may hold them co-responsible *if they do not act expeditiously to remove or disable access to information or services as soon as they become aware*, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information.[15]

These limitations on liability reflect the policy determination that exposing ICT intermediaries to liability for the conduct of users would create substantial barriers to innovation and would hinder the growth of the ICT sector.[16] If ICT intermediaries such as ISPs were exposed to criminal liability for the illegal conduct of their users, they would have to commit substantial resources to monitoring and policing their networks. Even where such monitoring is technically feasible (it often is not), the cost can be prohibitive. The threat of criminal liability can also close the market to innovative start-ups that cannot afford to pay for monitoring and compliance. Many ICT businesses choose not to operate in jurisdictions that refuse to limit their criminal liability for third party conduct.[17] The Asia Internet Coalition ("AIC"), an industry association founded by eBay, Google, Nokia, Skype, and Yahoo!, warns that imposing criminal liability on ICT intermediaries may result in denying Thai Internet users access to many of the online services they currently use on a daily basis.[18]

---

[13] Tunsarawuth and Mendel, note 2 above, at p. 6.

[14] Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, (Dec. 21, 2005), *available at* http://www.article19.org/pdfs/igo-documents/three-mandates-dec-2005.pdf.

[15] COE Declaration, note 5 above (emphasis added).

[16] *See* CDT memo on intermediary liability, note 12 above, at pp. 5-6.

[17] *See* CDT memo on intermediary liability, note 12 above, at pp. 5-6.

[18] *See* AIC Statement, note 12 above.

Several provisions of the Draft Bill, if broadly interpreted, would impose criminal liability on ICT intermediaries. Most notably, Section 22 makes it a crime to distribute, possess or publish software developed specifically to be used as a tool in the commission of offenses contained in Sections 15 through 20. If broadly interpreted, this might apply to an ISP that carries a message containing such software or to a web hosting service or a "cloud" storage provider whose users upload illegal software. Section 22 does not include any requirement that the intermediary have any knowledge of the unlawful software.

Similarly, Section 25 makes it a crime to "possess" computer data of an obscene nature relating to children or young people. To the extent that a web host or web forum that allows users to upload content "possesses" the uploaded content, the forum would be liable under Section 25 whenever a user uploads child pornography to the forum, even if the hosting service or forum had no knowledge of the unlawful content.

In the English translation we used for our analysis, Section 26 was unclear, but we are concerned that it might impose liability on intermediaries for content they did not create. It is a fundamental principle of Internet policy that intermediaries should not be held liable for content that they did not have actual notice of, and Section 26 should be revised if necessary to make it clear that it does not impose liability on Internet hosts, ISPs, or other technological intermediaries.

Overall, CDT recommends amending the Draft Bill to make it clear that ICT intermediaries are not liable for third party conduct. To address concerns with illegal content, the Bill could be amended to include a notice and takedown procedure, requiring Internet hosts to remove unlawful content posted by third parties after adequate notice and due process. ICT intermediaries that adhere to the takedown procedure and remove unlawful content upon adequate notice should not be subject to criminal liability.[19]

D. Procedural Safeguards for the Search and Seizure of Computer Systems and Data

The COE Convention recognizes "the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights . . ."[20]

To this end, parties to the Convention are required to ensure that the establishment, implementation and application of powers to search and seize computer systems and data are subject to procedural safeguards that shall "provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations [each state] has undertaken under

[19] For a brief overview of the concerns raised by notice and takedown, see CDT, "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation" (April 2010) p. 8, http://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_%282010%29.pdf.

[20] COE Convention, note 3 above, Preamble.

. . . the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments."[21]

Article 15 of the Convention goes on to state:

> Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include *judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure*.[22]

Although the Draft Bill takes steps to establish procedural safeguards similar to those contemplated by the COE Convention, our review of the search and seizure powers given to "Special Technical Officials" in Chapter 3 of the Draft Bill revealed a number of potential defects.

Section 31 of the Draft Bill states that special technical officials "[s]ubject to the provisions of Section 32," shall have various powers, including the power to copy computer data, inspect or access a computer system, and seize a computer system. Under Section 31, these powers may be exercised "for the benefit of investigation, in the case where there is reasonable evidence to believe that there is a commission of an offence according to this Act . . . [and] only as necessary, for the benefit of using as evidence of the commission of an offence and locating the offender."

Section 32 in turn establishes a set of procedural safeguards. Most importantly, it states that the officials, "[i]n applying the powers according to Section 31 . . . shall file a petition to a court with jurisdiction to request an order to permit special technical officials to execute according to the petition." Section 32 sets forth a number of requirements for the petition, including specification of "a reason for applying the powers, the manner of the commission of the offence, steps, methods, execution period and the impact or damage that may incur from the such application of powers." It also states the petition must contain "reasonable evidence to make believe that someone has committed or is going to commit certain act that is an offence according to this Act."

However, Section 32 does not clearly state that approval of the court reviewing the petition must be obtained before special technical officials can exercise any of the investigatory powers set forth in Section 31. We assume that the Section is intended to require such prior judicial approval, and the Thai language draft may be clearer than the translation we are relying on. We recommend that the drafters ensure that the Bill clearly states that each of the investigatory powers set forth in Section 31 can be exercised only after an independent and impartial judge from a court of competent jurisdiction so orders based on that judge's finding of reasonable cause. The Bill should clearly state that the judge's decision must be based on credible evidence presented in the petition.

---

[21] COE Convention, note 3 above, Article 15. The ICCPR, to which Thailand is a signatory, states in Article 17: "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks." UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, *available at* http://www.unhcr.org/refworld/docid/3ae6b3aa0.html.

[22] COE Convention, Article 15 (emphasis added).

We also note that Section 32 states that the investigatory power granted to special technical officials in Section 31(1)—the ability to copy computer data—"shall be executed only when there is reasonable cause to believe that an offence according to this Act has been committed, and it shall not excessively obstruct the operation of the owner or possessor of such computer data." There are no similar provisions in Section 32 with regard to the other three investigatory powers set forth in Section 31. We recommend that the Draft Bill be revised to make it clear that exercise of all the investigative powers in Section 31 should take into account the impact or damage to the owner or possessor of the computer systems and computer data, as well as to third parties, that may result from application of the powers.

III. Comments on Specific Provisions

With the above guiding principles in mind, we now comment on specific provisions in Chapter 2 of the Draft Bill.

Section 15

Section 15 of the Draft Bill states:

> Whoever wrongfully accesses a computer system or computer data of another person shall be punished with imprisonment not exceeding one year or fine not exceeding twenty thousand baht, or both.
>
> If the offence according to the first paragraph is committed to a computer system or computer data with a specific access prevention measure and that measure is not intended for his or her own use, it shall be punished with imprisonment not exceeding two years or fine not exceeding forty thousand baht, or both.
>
> If the offence according to the first or second paragraph is committed by using loopholes of a computer system or with copying computer data in a manner that is likely to cause damage to another person, it shall be punished with imprisonment not exceeding three years or fine not exceeding fifty thousand baht, or both.

As discussed above, CDT recommends that this provision be amended to include an intent element. Requiring intent for unlawful access offenses will bring the Draft Bill into greater alignment with the COE Convention[23] and the cybercrime laws of other nations.

Moreover, the drafters of the Bill must address the ambiguity of the phrase "wrongfully accesses." The word "wrongfully" is used throughout the Bill but is never defined. Cybercrime laws should be written with sufficient precision and clarity to enable computer users to determine from the face of the law what conduct is forbidden and what conduct is allowed, so that they can govern their behavior accordingly.

As written, Section 15 fails to provide individuals and businesses with adequate notice as to the kinds of access to computer systems and computer data of others that will be deemed

[23] *See* COE Convention, Article 2.

"wrongful." Because "wrongfully" is never defined, Section 15 and other provisions of the Draft Bill grant government officials excessively broad discretion to determine what conduct involving a computer system or computer data is criminal.

In particular, we are concerned that "wrongful access" could include using a computer service in ways prohibited by the terms of service. For example, Facebook expressly states in its terms of service that no one shall create an account on the site unless they are at least 13 years old. A twelve-year old who opens a Facebook account has violated that site's terms of service. Is she "wrongfully accessing" the computer hosting Facebook? The answer is unclear under the Bill as currently drafted, leaving too much discretion to prosecutors.[24] Unfortunately, the COE Convention is also flawed on this point and therefore provides no useful guidance.[25]

We note the contrast between the first sentence of Section 15 in the Draft Bill and Section 5 of the current CCA, which limits the concept of "wrongfully" accessing computer systems to those that have "specific security measure[s]." Thus, the CCA only criminalizes "wrongful" access to computer systems when it is done in circumvention of specific security measures. Section 15 of the Draft Bill removes this limitation. It allows prosecution for "wrongful" access to computer systems and computer data that have no security measures enabled and are therefore open to the public, while providing enhanced penalties for "wrongful" access to systems that have enabled "specific access prevention measure[s]."

Given these concerns about vagueness and overbreadth, CDT recommends that the first sentence of Section 15 be deleted. In place of the second sentence of Section 15, we propose language along the following lines, essentially equivalent to Section 5 of the CCA, as we understand it:

> Whoever wrongfully accesses a computer system of another person by intentionally circumventing a technical security measure and thereby obtains anything of value shall be punished with imprisonment not exceeding one year or fined not exceeding twenty thousand baht, or both.

---

[24] This is a problem that arises under the cybercrime laws of other nations, including the United States. Orin Kerr, a leading scholar of cyberlaw and a former official in the U.S. Department of Justice, has criticized the use of the undefined phrases "access" and "without authorization" in the U.S. statute. See Orin S. Kerr, Testimony before the U.S. House of Representative, Committee on the Judiciary. Subcommittee on Crime (November 15, 2011) http://judiciary.house.gov/hearings/pdf/Kerr%2011152011.pdf , and Orin S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes," NYU Law Review, vol. 78, no. 5, pp. 1596-1668 (November 2003) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740. In a recent article, Professor Kerr argued that the use of the phrase "without authorization" and the possibility that it can include terms of service makes the U.S. law unconstitutional under the principle that criminal statutes must clearly define the conduct they criminalize. Orin S. Kerr, "Vagueness Challenges to the Computer Fraud and Abuse Act," Minnesota Law Review (2010) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1527187.

[25] The illegal access provision of the COE Convention, Article 2, requires member states to adopt legislation that criminalizes intentional "access to the whole or any part of a computer system *without right*." (Emphasis added.) When the COE Convention was being drafted, it was criticized for failing to distinguish adequately between conduct that should be criminalized and conduct that, while violating contract or other laws, should not be criminalized. See "Comments of the Center for Democracy and Technology on the Council of Europe Draft 'Convention on Cyber-crime' (Draft No. 25)" (February 6, 2001), http://old.cdt.org/international/cybercrime/010206cdt.shtml. The Explanatory Report to the COE Convention addressed the problem of ambiguity in the phrase "without right" but failed to resolve it.

We believe that the term “technical security measure” may be more precise that the term “access prevention measure” used in the Draft Bill. If the phrase “specific access prevention measure” is used, it should be defined.

The third paragraph of section 15 introduces enhanced penalties for “wrongful” access to a computer system or computer data “by using loopholes of a computer system.” This clause, it seems, could be deleted, since “using loopholes” would be covered by the language we recommend above – “intentionally circumventing a technical security measure.”

Finally, Section 15 also introduces enhanced penalties for “wrongfully” accessing a computer system and “copying computer data in a manner that is likely to cause damage to another person.” The “likely to cause damage to another” standard, used in a number of the provisions of the Bill, is extremely broad. It gives government officials tremendous discretion to determine what constitutes “damage to another” and whether that damage is “likely” to occur. CDT recommends that the drafters limit this provision to obtaining “confidential data” or “non-public” data and by defining “damage” according to the specific types of harm that can stem from the unlawful access and copying of the data. This may include monetary loss or the harm caused by invasion of privacy. CDT further recommends that the provision include an intent element so that only those individuals who knowingly access and copy computer data with an intent to cause harm are subject to the enhanced penalties.

Section 19

Section 19 states:

> Whoever wrongfully commits any act to suspend, delay, hinder or disturb the working of a computer system of another person to the extent that it fails to work normally shall be punished with imprisonment not exceeding five years or fine not exceeding one hundred thousand baht, or both.

This section raises concerns because “fails to work normally” is undefined and extremely broad. The phrase can be applied to a wide range of changes to the operation of a computer system, including ordinary and innocent conduct such as installing a software program that has the incidental effect of reducing the computer’s operational speed. The provision grants government officials tremendous discretion to determine when a “wrongful” act has “disturbed” the “normal” functioning of a computer system.

Section 19 should be amended to require substantial harm to or impairment of the normal functioning of a computer system. Moreover, pursuant to the principle of intentionality discussed above, an intent element should be added so that only individuals who specifically intend to substantially harm or impair the normal functioning of a computer system are subject to prosecution.

Section 21

Section 21 states:

> If the commission of an offence according to Section 15, Section 16, Section 17, Section 18, Section 19 and Section 20
> (1) causes damage to the public, whether it be immediate or subsequent and whether it be synchronous or not, it shall be punished with imprisonment not exceeding ten years and fine not exceeding two hundred thousand baht
> (2) is an act that is likely to cause damage to security of the country, public safety, economic security of the country or public service, or is an act against computer data or a computer system available for public interest, it shall be punished with imprisonment of three to fifteen years and fine of sixty thousand to three hundred thousand baht.
> If the commission of an offence according to (2) causes the death of another person, it shall be punished with imprisonment of ten to twenty years.

The phrase "causes damage to the public" in Section 21(1) is unduly broad. The standard gives government officials unbridled discretion to determine what constitutes "damage to the public" and fails to provide Thai citizens with fair notice as to the types of conduct that will subject to them to the enhanced penalties. Under this provision, an individual guilty of "wrongfully" accessing the computer system of another person under Section 15 can be sent to prison for ten (10) years if a government official determines the illegal access caused "damage to the public." Such a penalty is draconian and likely contravenes international standards of proportionality in criminal punishment.[26]

Section 21(2) suffers from even greater vagueness, overbreadth, and potential disproportionality because government officials need only determine that a violation of Sections 15 through 20 is "likely" to cause damage to national security, "economic security," "public safety," or "public service" in order to establish a *minimum* prison sentence of three (3) years. Sections 21(2) also establishes a *minimum* prison sentence of three (3) years when a violation of Section 15 through 20 involves a computer system or computer data made "available for public interest." Thus, for example, by the terms of this section, an individual who violates Section 19 by disturbing the working of a computer in a Thai public library such that the computer "fails to work normally" is subject to a *minimum* prison sentence of three (3) years. This violates the principle of proportionality.

CDT recommends that the drafters of the Bill strike Section 21 in its entirety.[27]

---

[26] Article 9 of the International Covenant on Civil and Political Rights ("ICCPR"), to which Thailand is a signatory, requires that deprivations of liberty be proportionate to the offense committed.

[27] The final provision of Section 21, imposing a prison term of ten (10) to twenty (20) years for violations of Section 15 – 20 and Section 21(2) that "cause[] the death of another person" is adequately addressed by the Penal Code's murder provisions.

Section 22

Section 22 states:

> Whoever makes, sells, distributes, copies, possesses or publishes by any manner computer data, sets of instructions or equipment developed specifically to be used as tool in the commission of an offence according to Section 15, Section 16, Section 17, Section 18, Section 19 and Section 20 shall be punished with imprisonment not exceeding one year or fine not exceeding twenty thousand baht, or both.

As noted above, Section 22 should be revised to protect ICT intermediaries from criminal liability for merely distributing, copying, possessing, or publishing unlawful software tools when those tools are uploaded by third party users without the actual knowledge of the ICT intermediary. In addition, this section should require that violators *knowingly* distribute the unlawful software tools and equipment with a specific intent that the tools be used to commit an offense according to Sections 15 through 20.

Section 23

Section 23 states:

> Whoever commits an offence according to the following shall be punished with imprisonment not exceeding five years or fine not exceeding one hundred thousand baht, or both:
> (1) importing to a computer system data contrary to truth in a manner that is likely to cause damage to security of the country or cause public panic;
> (2) importing to a computer system any computer data that is an offence relating to the security of the Kingdom or an offence relating to terrorism according to the Penal Code;
> (3) disseminating or forwarding computer data already known to be computer data according to (1) or (2).

The "contrary to the truth" standard of Section 23(1) is unworkable and does not appear to protect any legitimate interest. The standard leaves total discretion with Thai officials to determine what constitutes true data, and therefore what data is "contrary to the truth." Moreover, these same officials are granted unrestrained discretion to determine when "untrue" data imported into a computer system is "likely" to "damage" national security or cause "public panic." Similar laws criminalizing the dissemination of false information likely to cause "public panic" have been struck down as unconstitutional violations of the freedom of expression in other countries.[28] Section 23(1) provides altogether too much discretion to government officials and fails to provide adequate notice to Thai computer users as to the types of conduct that run

[28] *See* Chavunduka & Choto v. Minister of Home Affairs & Attorney General, 22 May 2000, Judgement No. S.C. 36/2000, Civil Application No. 156/99 (Supreme Court of Zimbabwe) and R. v. Keegstra [1990] 2 SCR 697 (Supreme Court of Canada).

afoul of the law. CDT recommends that the drafters of the Bill eliminate the provision in its entirety.

With respect to Section 23(2), the principle of technology neutrality discussed above applies. In general, there is no need to create special penalties for crimes already recognized in the Penal Code merely because they involve computers. When the importation of computer data into a computer system constitutes a national security or terrorism offense under the Penal Code, it should be punished under the Penal Code.

Section 24

Section 24 states:

> Whoever imports to a computer system that the public may access computer data of obscene nature and without an access prevention measure for children and young people shall be punished with imprisonment of three to fifteen years or fine of sixty thousand to three hundred thousand baht, or both.

In order to provide computer users and ICT intermediaries with sufficient notice regarding the types of conduct that run afoul of this provision, "computer data of obscene nature" and "access prevention measure" should be clearly defined.

Section 27

Section 27 states:

> Whoever imports to a computer system that the public may access computer data appearing in picture, personal data of another person or other data in a manner likely to cause damage to another person, impair his or her reputation, expose him or her to hatred, contempt or embarrassment, or to deceive any person to be true data shall be punished with imprisonment not exceeding three years or fine not exceeding one hundred thousand baht, or both.
>
> The offences in the first paragraph are compoundable offences.
>
> If the injured person in the offences in the first paragraph dies, the father, mother, spouse or child of the deceased shall have the power to administer on his or her behalf and shall be deemed that such person is the injured person according to the Criminal Procedure Code mutatis mutandis.

The principle of technology neutrality discussed above applies to Section 27. The existing defamation provisions of Thai law are sufficient to protect Thai citizens from defaming materials imported into publicly accessible computer systems. CDT recommends that the drafters of the Bill strike Section 27 in its entirety.

Section 34

Section 34 allows special technical officials to request a court order to prohibit the sale or dissemination of an "undesirable set of instructions" or to impose other limits on an owner or possessor of data containing such instructions. Section 34 defines undesirable sets of instructions as "a set of instructions that causes computer data or a computer system or other sets of instructions to damage, destroy, revise or add, disrupt or operate in contrary to instructions that have been set . . . ."

CDT believes this definition is overbroad and risks criminalizing innocent conduct of computer users. Greater precision can be achieved by applying the principle of intentionality. Undesirable instructions should be defined as instructions specifically designed to cause damage, destroy, or disrupt computer systems or computer data.

IV. Conclusion

It is appropriate to adopt a new cybercrime bill to replace the 2007 CCA. However, the Draft Bill does not go far enough in clarifying the ambiguities of the CCA and harmonizing Thai cybercrime law with international standards.

In the interests of Thailand's global economic competitiveness in information and communications technologies, the Bill should be amended in accordance with the guiding principles and specific recommendations discussed above.

For further information, contact Cynthia Wong, Director of CDT's Project on Global Internet Freedom, cynthia@cdt.org, or James X. Dempsey, Vice President for Public Policy, jdempsey@cdt.org.

English Translation of the Draft Bill Used in CDT Analysis

Computer-Related Offences Commission Act
B.E. _____ (_____)

_____

……
……
……

as it is deemed appropriate to amend the law governing the commission of a computer-related offence.

…….

Section 1 This Act shall be called the "Computer-Related Offences Commission Act B.E. _____ ".

Section 2 This Act shall come into force 30 days following the date of its publication in the Royal Gazette.

Section 3 The Computer-Related Offences Commission Act B.E. 2550 (2007) shall be repealed.

Section 4 In this Act,

"Computer System" means equipment or sets of equipment of computer, whose function is integrated together, for which instructions, sets of instructions or other things, and working principles are set to enable equipment or sets of equipment to perform the duty of processing data automatically, including other electronic equipment of similar nature.

"Computer Data" means data, statements, instructions, sets of instructions or other things that may be processed by a computer system, and shall also include electronic data according to the law of electronic transactions.

"Computer Traffic Data" means data relating to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, periods of time, types of services or others relating to such computer system's communications.

"Service Provider" means:

(1) A person who provides services to other persons in accessing the Internet or in allowing them to communicate to each other by other means via a computer system, whether on his or her own behalf or in the name of or for the benefit of other persons;

(2) A person who provides services of storing computer data for the benefit of other persons.

"Service User" means a person who uses services of service providers with or without a fee.

"System Caretaker" means a person entitled to access a computer system that provides services to other persons in accessing the Internet, or in allowing them to communicate to each other by other means via a computer system, whether in caretaking for his or her own benefit or for the benefit of other persons.

"Committee" means Prevention and Suppression of Computer-Related Offences Committee.

"Minister" means a Minister who has the responsibility and control for the execution of this Act.

Section 5 The Minister of Information and Communication Technology shall have responsibility and control for the execution of this Act and shall have the power to issue ministerial rules for the purpose of the execution of this Act.

Ministerial rules shall be enforceable upon its publication in the Royal Gazette.

Chapter 1
Prevention and Suppression of Computer-Related Offences Committee

Section 6 There shall be a committee called "Prevention and Suppression of Computer-Related Offences Committee" consisting of the Prime Minister as the chairman, the Minister of Information and Communication Technology as the vice chairman, the Minister of Justice, the Minister of Defence, the Minister of Finance, the National Police Commander, the Secretary General of the National Security Council, the Director of the National Intelligence Agency and three qualified members whom the cabinet appoints by identifying from persons having the apparent knowledge, expertise and experience in the fields of law, science, engineering, banking and finance, or social science.

Qualified members shall hold office for four years in a term.

Representatives from the Office of Electronic Transaction Development; the Office of Supervision of Information Technology Application; the Office of Technology Cases, Department of Special Investigation; the group of inspecting and analyzing commission of technological offences, Technology Support Division shall jointly be the secretary.

Section 7 The Prevention and Suppression of Computer-Related Offences Committee shall have the following powers and duties:

(1) to propose recommendations to the cabinet in forming policies of prevention and suppression of computer-related offences, including the solving of relating problems and obstacles;

(2) to monitor and oversee the prevention and suppression of computer-related offences;

(3) to issue regulations or notifications according to this Act;

(4) to summon any person to give statements, to deliver relevant documents or evidence or other things for deliberation;

(5) to perform any other act according to this Act or other laws.

In the performance according to this Act, the Committee shall have the power to appoint sub-committees to perform as the Committee assigns. Provisions according to Section 10 to Section 14 shall apply to meetings of sub-committees mutatis mutandis.

The Committee and sub-committees shall be an official according to the Penal Code.

Section 8 In addition to the vacation of office upon the expiry of the term, a qualified member vacates office upon:

(1) death;

(2) resignation;

(3) being a bankrupt;

(4) being an incompetent or quasi-incompetent person

(5) having been imprisoned by a final judgment to a term of imprisonment except for a petty offence or an offence committed through negligence;

(6) the Committee passing a resolution unanimously removing him or her from office because of behaving or having used to behave severely degrading or being defective to good morals.

Section 9 In the case where a qualified member vacates office before the expiry of his or her term, persons with the power of appointment may appoint another person as the replacement. The replacement person appointed shall hold office for the remaining term of the member he or she replaces.

In the case where a member is appointed in addition to members whose term still remains, the additional appointed member shall hold office for the remaining term of the incumbent members.

Section 10 Meetings of the Committee shall consist of at least one half of the members to meet the quorum.

In the case where the number of members meets the quorum, but the deliberation of any issue that is postponed from the previous meeting because lack of quorum, if a meeting of such issue is called again within fourteen days from the day of postponement and there are at least one-thirds of the total number of members at the latter meeting, the quorum shall be met. But the objectives to have the effect of this provision shall be specified in the letter calling for such meeting.

Section 11 Any calling for a meeting shall be executed in writing and shall be notified to all members at least three days in advance, except for members who are already notified of such calling at a meeting. In such a case, letters calling for a meeting may be notified only to members absent from the meeting.

Provisions according to the first paragraph shall not apply to cases of urgency where the chairman may call a meeting in a different manner.

Section 12 The chairman shall have the powers and duties in executing meetings, and for keeping orders at meetings, the chairman shall have the power to give any order as necessary.

If the chairman is not present at a meeting or cannot perform his duties, the vice chairman shall perform his duties instead. If there is no vice chairman or there is one but he or she cannot perform the duties, members present at the meeting shall select one member to perform instead.

In the case where the chairman has the duties to execute any other act in addition to executing meetings, provisions in the second paragraph shall apply mutatis mutandis.

Section 13 Any voting at a meeting shall be executed by a simple majority.

A member shall have one vote. If the votes are equal, the chairman at the meeting shall execute an additional vote as the final vote.

If there is no opponent in any issue, the chairman shall ask the meeting whether there is anyone with a different view. If there is no different view, it shall be deemed that the meeting votes to approve such issue.

Section 14 Meetings shall produce meeting reports in writing.

If there is any opposing view, such opposing view shall be recorded together with the reasons in meeting reports. If members in the minority propose any opposing view in writing, such opposing view shall also be recorded.

Chapter 2
Computer-Related Offences

Section 15 Whoever wrongfully accesses a computer system or computer data of another person shall be punished with imprisonment not exceeding one year or fine not exceeding twenty thousand baht, or both.

If the offence according to the first paragraph is committed to a computer system or computer data with a specific access prevention measure and that measure is not intended for his or her own use, it shall be punished with imprisonment not exceeding two years or fine not exceeding forty thousand baht, or both.

If the offence according to the first or second paragraph is committed by using loopholes of a computer system or with copying computer data in a manner that is likely to cause damage to another person, it shall be punished with imprisonment not exceeding three years or fine not exceeding fifty thousand baht, or both.

Section 16 Whoever knows the means to intrude a computer system or computer data with an access prevention measure created specifically by another person, if wrongfully disclose such means in a manner that is likely to cause damage to another person, shall be punished with imprisonment not exceeding one year or fine not exceeding twenty thousand baht, or both.

Section 17 Whoever wrongfully commits any act by electronic means or by using sets of instructions to eavesdrop computer data of another person shall be punished with imprisonment not exceeding three years or fine not exceeding sixty thousand baht, or both.

Section 18 Whoever wrongfully damages, destroys, revises, changes, adds, degrades or makes useless in whole or in part computer data of another person shall be punished with imprisonment not exceeding five years or fine not exceeding one hundred thousand baht, or both.

Section 19 Whoever wrongfully commits any act to suspend, delay, hinder or disturb the working of a computer system of another person to the extent that it fails to work normally shall be punished with imprisonment not exceeding five years or fine not exceeding one hundred thousand baht, or both.

Section 20 Whoever sends computer data or electronic mail for trading interest to the extent that it causes trouble or annoyance to another person without allowing the receiver of computer data or electronic mail to unsubscribe or notify his wishes to reject its receipt shall be punished with imprisonment not exceeding six months or fine not exceeding ten thousand baht, or both.

Section 21 If the commission of an offence according to Section 15, Section 16, Section 17, Section 18, Section 19 and Section 20

(1) causes damage to the public, whether it be immediate or subsequent and whether it be synchronous or not, it shall be punished with imprisonment not exceeding ten years and fine not exceeding two hundred thousand baht

(2) is an act that is likely to cause damage to security of the country, public safety, economic security of the country or public service, or is an act against computer data or a computer system available for public interest, it shall be punished with imprisonment of three to fifteen years and fine of sixty thousand to three hundred thousand baht.

If the commission of an offence according to (2) causes the death of another person, it shall be punished with imprisonment of ten to twenty years.

Section 22 Whoever makes, sells, distributes, copies, possesses or publishes by any manner computer data, sets of instructions or equipment developed specifically to be used as tool in the commission of an offence according to Section 15, Section 16, Section 17, Section 18, Section 19 and Section 20 shall be punished with imprisonment not exceeding one year or fine not exceeding twenty thousand baht, or both.

Section 23 Whoever commits an offence according to the following shall be punished with imprisonment not exceeding five years or fine not exceeding one hundred thousand baht, or both:

(1) importing to a computer system data contrary to truth in a manner that is likely to cause damage to security of the country or cause public panic;

(2) importing to a computer system any computer data that is an offence relating to the security of the Kingdom or an offence relating to terrorism according to the Penal Code;

(3) disseminating or forwarding computer data already known to be computer data according to (1) or (2).

Section 24 Whoever imports to a computer system that the public may access computer data of obscene nature and without an access prevention measure for children and young people shall be punished with imprisonment of three to fifteen years or fine of sixty thousand to three hundred thousand baht, or both.

Section 25 Whoever possesses computer data of obscene nature relating to children or young people shall be punished with imprisonment not exceeding six years or fine not exceeding two hundred thousand baht, or both.

Section 26 Any service provider or system caretaker willful or consenting to the commission of an offence according to Section 23 and Section 24 in a computer system under his or her control shall be punished as the same to the person committing the offence under Section 23 and Section 24.

Section 27 Whoever imports to a computer system that the public may access computer data appearing in picture, personal data of another person or other data in a manner likely to cause damage to another person, impair his or her reputation, expose him or her to hatred, contempt or embarrassment, or to deceive any person to be true data shall be punished with imprisonment not exceeding three years or fine not exceeding one hundred thousand baht, or both.

The offences in the first paragraph are compoundable offences.

If the injured person in the offences in the first paragraph dies, the father, mother, spouse or child of the deceased shall have the power to administer on his or her behalf and shall be deemed that such person is the injured person according to the Criminal Procedure Code mutatis mutandis.

Section 28 Any system caretaker uses his or her duty to commit an offence according to Section 15, Section 16, Section 17, Section 18, Section 19, Section 20 and Section 22 shall be liable to an increase of one half of the punishment provided for in such Section.

Section 29 Whoever committing an offence according to this Act outside the Kingdom and

(1) the offender be a Thai person and there be a request for punishment by the government of the country where the offence has occurred or by the injured person; or

(2) the offender be an alien and the Thai government or a Thai person be the injured person and there be a request for punishment by the injured person

shall be punished in the Kingdom.

Chapter 3
Special Technical Officials

Section 30 In the case where there is need to coordinate with foreign agencies in acquiring data that is useful for investigation, investigative officials shall request the Office of Electronic Transaction Development to be the coordinator in acquiring such data.

Section 31 Subject to the provisions of Section 32 and for the benefit of investigation, in the case where there is reasonable evidence to believe that there is a commission of an offence according to this Act, special technical officials shall have any of the following powers, only as necessary, for the benefit of using as evidence of the commission of an offence and locating the offender:

(1) copy computer data, computer traffic data from a computer system, in which there is reasonable cause to believe that an offence according to this Act has been committed, in case such computer system is not yet in the possession of special technical officials;

(2) inspect or access a computer system, computer data, computer traffic data or equipment for storing computer data belonging to any person that is evidence of or may be used as evidence relating to the commission of an offence or for the investigation to locate the offender, and order such person to send, only as necessary, any relating computer data, computer traffic data;

(3) decode password of computer data of any person or order any person relating to coding of password of computer data to decode or cooperate with special technical officials in such decoding;

(4) attach a computer system, only as necessary, specifically for the benefit of knowing details of an offence and an offender according to this Act.

Section 32 In applying the powers according to Section 31, special technical officials shall file a petition to a court with jurisdiction to request an order to permit special technical officials to execute according to the petition. The petition must specify a reason for applying the powers, the manner of the commission of the offence, steps, methods, execution period and the impact or damage that may incur from such application of powers, including details of equipment relating to the commission of the offence and the offender, as much as it can be identified. There shall also be reasonable evidence to make believe that someone has committed or is going to commit certain act that is an offence according to this Act, in accompanying the petition. The court shall adjudicate such petition urgently.

The court shall have the power to hear any relating person before its adjudication on such matter, except in case of necessity and urgency, the court may adjudicate unilaterally.

When the court gives its order of permission, before executing according to such order of the court, special technical officials shall submit a copy of the note that records the reason for applying the powers according to Section 31 to the owner or possessor of such computer system as evidence thereof. If there is no owner or possessor of computer sets at the place, special technical officials shall submit a copy of such note to such owner or possessor as soon as possible.

The special technical official who is the chief of the execution according to Section 31 shall submit a copy of the note that records details of the execution and reasons of the execution to the court with jurisdiction within forty eight hours from the beginning of the execution as evidence thereof.

In copying computer data according to Section 31 (1), it shall be executed only when there is reasonable cause to believe that an offence according to this Act has been committed, and it shall not excessively obstruct the operation of the owner or possessor of such computer data.

In attaching according to Section 31 (4), apart from submitting a copy of the letter of attachment to the owner or possessor of such computer system as evidence thereof, special technical officials shall not attach exceeding thirty days. In case of necessity to attach for a longer period of time, a petition to extend the attachment period shall be filed with a court with jurisdiction. The court may permit for one or several extensions, but the total period shall not exceed another sixty days. When the necessity of attachment is

no longer the case or such period of time expires, special technical officials must withdraw the attachment of such computer system immediately.

The letter of attachment according to the sixth paragraph shall be in accordance with a ministerial rule.

Section 33 In the case where the commission of an offence according to this Act is the dissemination of computer data that may have an impact on the security of the Kingdom as stipulated in Book 2 Title 1 or Title 1/1 of the Penal Code, or that is contrary to public order or good morals according to this Act or other laws, special technical officials with the approval from the Minister may file a petition with a court with jurisdiction to request an order to terminate such dissemination of computer data. The petition must specify a reason for applying the powers, the manner of the commission of the offence, steps, methods, execution period and the impact or damage that may incur from such termination of dissemination. There shall also be reasonable evidence to make believe that someone has committed or is going to commit certain act that is an offence according to this Act, in accompanying the petition.

In the case where the court issues any order to terminate the dissemination of computer data according to the first paragraph, special technical officials shall execute such termination of dissemination themselves or order a service provider to terminate the dissemination of such computer data.

The special technical official who is the chief in the execution according to the second paragraph shall submit a copy of the note that records details of the execution and reasons of the execution to the court with jurisdiction within forty eight hours from the beginning of the execution as evidence thereof.

Section 34 In the case where special technical officials find out that any computer data contains an undesirable set of instructions, special technical officials may file a petition with a court with jurisdiction to request an order to prohibit the sale or dissemination or order the owner or possessor of such computer data to terminate the use, destroy or revise such computer data, or may set conditions for the use, possession or dissemination of such undesirable set of instructions.

An undesirable set of instructions according to the first paragraph means a set of instructions that causes computer data or a computer system or other sets of instructions to damage, destroy, revise or add, disrupt or operate in contrary to instructions that have been set, or any other effects stipulated in a ministerial rule, except for a set of instructions that aims to prevent or revise aforementioned sets of instructions as stipulated by the Minister in the Royal Gazette.

Section 35 Special technical officials shall not disclose or deliver computer data, computer traffic data or data of a service user acquired according to Section 31 to any other person.

Provisions according to the first paragraph shall not apply to any act executed for the benefit of prosecution of an offender according to this Act or for the benefit of prosecution of a special technical official relating to wrongful exercise of powers.

In case of necessity and for the benefit of justice, special technical officials may file a petition to the court to request the use of computer data, computer traffic data or data of a service user for the benefit of prosecution according to other laws. But the rights and liberty of other persons must not be affected unreasonably.

Any special technical official who violates the first paragraph shall be punished with imprisonment not exceeding three years or fine not exceeding sixty thousand baht, or both.

Section 36 Any special technical official by negligence causes any other person to know computer data, computer traffic data or data of a service user acquired according to Section 24 shall be punished with imprisonment not exceeding one year or fine not exceeding twenty thousand baht, or both.

Section 37 Whoever knows computer data, computer traffic data or data of a service user acquired by special technical officials according to Section 31 and disclose such data to any other person shall be punished with imprisonment not exceeding two years or fine not exceeding forty thousand baht, or both.

Section 38 Data, computer data or computer traffic data that special technical officials acquire according to this Act shall be admissible as evidence according to provisions of the Criminal Procedure Code or other laws relating to investigation of evidence. But it must not be the way of persuasion, promising, coercion, deceiving or other wrongful means.

Section 39 A service provider must keep computer traffic data for no less than ninety days from the day such data enters a computer system. But in case of necessity, special technical officials may order any service provider to keep computer traffic data for longer than ninety days but not exceeding one year on a special case-by-case basis and on a specific occasion.

A service provider must keep data of a service user as much as necessary in order to be able to identify the service user from the beginning of the use of service and must keep for no less than ninety days from the end of the use of service.

That the provisions according to the first paragraph shall apply to any kind of service providers, by how and when shall be in accordance with an announcement of the Minister in the Royal Gazette.

Any service provider who fails to comply with this Section shall be punished with fine not exceeding five hundred thousand baht.

Section 40 Whoever fails to comply with any order of the court or special technical officials issued according to Section 31 or Section 33 or fails to comply with an order of the court according to Section 34 shall be punished with fine not exceeding two hundred thousand baht and additional daily fine not exceeding five thousand baht until the compliance.

Section 41 In appointing special technical officials according to this Act, the Minister shall appoint from persons the Committee nominates in a list of persons with knowledge and expertise relating to computer system and having the qualifications as stipulated by the Minister.

Section 42 In the performance of duties according to this Act, special technical officials shall be an official according to the Penal Code.

When finding or believing that an offence according to this Act has been committed, an investigative official shall coordinate with special technical officials for assistance in investigating for relating offenders and evidence.

Section 43 In the performance of duties, special technical officials must produce an identification card to any relating person.

An identification card of special technical officials shall be in accordance with a form that the Minister announces in the Royal Gazette.

Countersigned
……
Prime Minister