University of Washington (UW) - Google Intermediary Liability Research Project: Online Intermediary Liability and Privacy Protection in Thailand

Abstract

In Thailand, online data protection is a new and unfamiliar topic for Thai people. However, it is necessary to raise awareness among the people of Thailand regarding this topic as it has become increasingly difficult to draw a demarcating line between the right of privacy, public interest, and national security. In order to do so, this paper will discuss on the issue of liability of the internet intermediary under Thai laws. In addition, it will point out the tension between the liability of internet intermediaries, the freedom of speech, and the freedom of expression. Moreover, it will analyze the appropriateness of the draft legislation which is related to the issue of privacy right.

Authors' Biography

Assistant Professor Dr. Bhumindr Butr-Indr has obtained his Ph.D. in Intellectual Property from Université Panthéon Assas (Paris II) in 2012. He completed his LL.M. (Master of Law) in 2006 from L'Université Paul Cézanne (Aix-Marseille 3) in France. In addition, he gained a Barrister at Law since 2003 from the Institute of Legal Education, Thai Barrister Association. Dr. Butr-Indr received an LL.B. (Bachelor of Laws) in 2001 from Thammasat University. At present, he is a lecturer at Thammasat University, Thailand. Apart from his teaching at Thammasat University, Dr. Butr-Indr has taught law at other Universities and worked as legal counsel for the Public Health Ministry in Thailand. Moreover, he is a qualified expert in Intellectual Property Law of the Department of Disease Control (Ministry of Public Health) and the Department of Intellectual Property (Ministry of Commerce). Dr. Butr-Indr is also a consultant for the Thai government departments, the private sector and international organisations. He has published over 15 academic books and journals in the areas of the law on Intellectual Property Rights, Business law, and International Investment law.

Wassamon Kun-amornpong is a law lecturer at Thammasat University, Thailand. She was a recipient of the Royal Thai Government scholarship to study law abroad. She obtained her LL.M. from UCLA School of Law, Los Angeles, U.S.A. in 2008 and LL.B. (Bachelor of Laws) in 2007 from the London School of Economics and Political Science (LSE), London, U.K. Her academic interests are Comparative Civil Laws, Jurisprudence, Information Technology Law, and Financial Regulation. She was also a vice-director for Mekong Region Legal Studies Program at Thammasat University, Thailand.

Taenrat Kunngern was a graduate of La Trobe University, Melbourne, Australia where he completed his LL.M. (Master of Global Business Law). He has an LL.B. (Bachelor of Laws) from Khon Kaen University, Thailand. Mr. Kunngern has two years of teaching experience in the areas of Business Law, Contract Law, and Civil Law at Khon Kaen University. Prior to joining the Faculty of Law at Khon Kaen University, he worked for the local firm (Nitirat Law Firm) in the position of contract drafter assistant and consultant on the business law cases.

TABLE OF CONTENTS

Introduction

The right to privacy has increasingly become an important concept in Thai society. Its importance has manifested by the fact that the right to privacy has been written explicitly into many of previous Constitutions of the Kingdom of Thailand. For example, Article 34 of the Thai Constitutions B.E. 2540 and Article 35 of the Thai Constitution B.E. 2550 have mentioned that:

> "[A] person's family rights, dignity, reputation or the right of privacy shall be protected. The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which is beneficial to the public."[1]

These Articles, which have their roots from the contents of the Universal Declaration of Human Rights[2], have demonstrated the fact that Thailand has given a high priority to the status of human rights including the right to privacy.[3]

The concept of privacy right in Thai laws has been significantly influenced by the German theory as a fundamental right.[4] German theorists have continued to develop this concept in order to create a protection for the people from a draconian regime of, for example, Adolf Hitler which more than 20 million people were killed in genocide. Hence, the Basic Law[5] has firmly embraced the principles of fundamental rights within it.[6] It cause the German legal system has an advanced principle which could fill in the gap in the case that there are arising concerns due to the

---

[1] The right to privacy was also mentioned in other previous constitutions (e.g. the Constitution of Thailand B.E. 2534). In addition, it was stated in the recently-dismissed Draft Constitution of Thailand B.E. 2558 (in Thai), http://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/download/article/article_20150429103838.pdf.

[2] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (Dec.10, 1948).

[3] *See Id.* art.12 "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to at tacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

[4] Cf. Dieter Grimm, Die Entwicklung der Grundrechtstheorie in der deutschen Staatsrechtslehre des 19. Jahrhunderts, in Dieter Grimm, Recht und Staat der bürgerlichen Gesellschaft 308 (1987); Walter Pauly, Der Methodenwandel im deutschen Spätkonstitutionalismus (1993).

[5] Basic Law for the Federal Republic of Germany [Germany], 23 May 1949, available at: http://www.refworld.org/docid/4e64d9a02.html [accessed 7 November 2017]

[6] On the importance of German constitutional jurisprudence, see David Robertson, The Judge as a Political Theorist (2010).

changing society regarding fundamental rights which have not been written into the Basic Law for the Federal Republic of Germany.[7] Privacy rights are under the umbrella of the public right of way (subjective-öffentliche Rechte). There are three dimensions of fundamental rights including status negativus, status positivus, and status activus.[8] The right to privacy is categorized into the dimension of status negativus, which protects an individual's rights and liberties from being infringed by a government act without that person's consent.

However, the situation of privacy right in Thailand has become increasingly alarming as Thailand is facing one of the most difficult periods of time in the country's history. There was a military coup in 2014 and the country is still governed by the authoritarian government. There are two main factors which demonstrate the worrying situation of privacy right in Thailand. First, there is only one governmental organization in Thailand, the National Human Rights Commission of Thailand (NHRCT), which has a constitutional duty to protect human rights. However, the NHRCT has no enforcement power to punish those who infringe on human rights. The authority is only limited to reporting cases concerning human rights to the Constitution Court.

Second, the military coup in 2014 has led the country to be governed under an authoritarian regime. Under the current regime, it is not difficult for the government to infringe upon the citizen's privacy right. In other words, the right to privacy is limited far beyond other democratic societies. For instance, the military government supports the policy of absolute control on internet use by limiting the internet gateway. This policy is known as "Single Gateway" which is a hotly debated issue at the moment in Thailand. The government has argued that the rationales of this policy are the protection of national security and the prohibition of illegal websites.

Nevertheless, in practice, once this policy is legally approved and takes effect, the government will have a legal right to get access to personal information of its subjects on the internet. This means that the citizens will no longer be able to keep their personal information away from the prying eyes of the government. Personal data on the internet would be available for the use by the government. Besides, it is insecure for the people at large since the practice of getting access to personal data will be subject to subjective discretion of the government officials. This might

[7] *See id.*
[8] Klaus F. Röhl, Allgemeine Staatslehre, Köln-Berlin-Bonn_ *München: Carl Heymanns, 1995, S. 349.*

finally lead to a situation of no guarantee to privacy right of the citizens at all. Furthermore, Thai people might have no opportunity to receive true information regarding the government's exercise of the state power.

In this paper, the authors will analyze the legal framework regarding the protection of the right to privacy in Thailand. The research consists of three parts. Part I will provide the backgrounds of the concept of privacy, the right to privacy in Thai legislation, and the personal data of Thai citizens on the internet. Part II will describe liability resulting from the intrusion of privacy under Thai law. Part III will analyze the appropriateness of the draft legislation relating to privacy rights in Thailand.

Part I: The Concept of Privacy Right

The right to privacy is under the umbrella of human rights, which guarantee that the privacy will be protected by the law.[9] Privacy right protection ensures that people can live their lives while maintain their freedom and equality with other people in the society. The boundaries of an individuals' right is legally drawn in order to prevent a person from unwanted interference by others. The function of these boundaries includes the protection of a person from being harmed physically or mentally.[10] In addition, a person is entitled to defend his or her reputation as everyone has equal human dignity according to art 1 of the Universal Declaration of Human Rights.[11] The privacy right is a highly prized part of natural rights, even above other values (e.g. morality, ethics, and social tradition). Moreover, diversity in the society is one of the factors which affect rights of the individual and it can be argued that privacy right stems from cultural and social practice of the people in a particular society.

[9] Cranston, Maurice. Human Right To-Day, London, Ampersand book, 1962.
[10] Who Does Regulate the New World?: A Case Study on the Internet, Bangkok, The Foundation of Internet and Civil Culture, 2015.
[11] "All human begins are born free and equal in dignity and rights …", *supra* note 2.

A. Definition of Privacy Right

It is widely acknowledged that human beings are social animals. When there is a gathering of human beings, a society is formed. In order to maintain the peace in the society, there must rules to control people who live within it. However, the form and degree of severity of the rules are various depending on how much people pay respect towards others. The rules which are needed might be a standard rule or social contract that all members in the society willingly accept and follow it. In addition, there will be a need to determine the status and duty of the leader in order to rule the society. However, there are some activities of the individuals with which the state or the ruler should not interfere without the individuals' consent. This private sphere and the activities therein form the boundaries of privacy.[12]

In some countries, the concept of a privacy right is interpreted to completely cover the area of personal data protection. Moreover, the right to privacy has expanded to cover other related rights (e.g. information privacy[13], bodily privacy[14], communication privacy[15], territorial privacy[16]).[17] Although there are many types of privacy rights protection, many countries place a high priority on personal data protection, among others. This is due to the development of information technology and advanced computer systems. Nowadays, communication and dissemination of information can be done regardless of time and place. The collection, processing, and disclosure of information can be performed easily. However, this increases the risk that the database of personal information will be hacked or used illegally.

B. The Forms of Privacy Right Protection

According to the abovementioned situation, the protection of privacy right has become increasingly important. Many countries have implemented measures in order to prevent the

[12] Chuendaree Maleepraserch, Privacy rights with communication: The Protection of Right to Privacy and the Communication of Information, Thailand, Chulalongkorn University, 1996.
[13] The protection of data lays down the principle regarding the management and collection of personal information.
[14] Physical body shall not be infringed in a non-humanitarian manner.
[15] People should have freedom in communication. Their communication should not be disturbed or spied by others.
[16] It is the right to impose restriction that people who have no permission shall not intrude into a person's private place.
[17] Cranston, Maurice, Human Right To-Day, London, Ampersand book, 1962.

violation of privacy right by using personal data or information without any explicit consent of the data owner. These measures are in the forms of general legislation, specific legislation or self-governance.[18]

(1) General Legislation

Most countries have passed law concerning the collection, disclosure, and utilization of personal information in the public and private sectors. In the industrial sector, a company may create some departments which have complete authority to lay down and enforce principles regarding privacy right.

(2) Specific Legislation

Some countries including the United States of America use this method. They do not enact the legislation which provides privacy right protection in general.[19] There are specific laws to regulate behavior of the people in this area (e.g. the law regarding financial information collection). However, there are some limitations in using this method. First, law enforcers in this regime have to coordinate with many governmental departments in order to apply the law to cases before them. Second, there is no central organization or department which could lead or take direct responsibility for this issue. Therefore, the protection of privacy right might be cumbersome.

(3) Self-governance

In theory, personal data may be protected by using the measure of self-regulation. This means the private sector is to regulate itself. However, there is a risk of relying on the discretion of the private sector as there is no guarantee that the privacy right will be protected in a manner which is both ethical and efficient. For example, a company might sacrifice the protection of the privacy right if that means its business could survive in a fierce competition.

[18] Thai Information Law (Nov. 4, 2016), http://www.no-poor.com/inttotocomandcomapp/rule.html

[19] The Third Amendment stems from the anger colonists felt when the King of England forced them to house military troops, even in times of peace. Although not a problem in recent times, the Supreme Court has held that the Third Amendment's prohibition against the quartering of soldiers "in any house in time of peace without the consent of the owner" is the foundation of the right to privacy. Thus, while the Constitution does not specifically provide for a right to privacy, the First, Third, Fourth, and Fifth Amendment create "zones of privacy" around a citizen's property and person.

C. The Development of Personal Data Protection

Since the 1960s and 1970s, the protection of privacy right has taken an increasingly important role because of the progress and advancement of the information technology. At present, computer system and networking technology have developed rapidly. In addition, computer application and services can be accessed more easily. Efficiency in processing and retrieving computer data makes it necessary to create a law in order to regulate these activities and prevent the privacy right violation.[20]

There are two international organizations which have a duty to formulate law regarding privacy protection. One of them is the Council of Europe which has established the Convention for the Protection of Individual with regard to the Automatic Processing of Personal Data (1981).[21] The other one is the Organization for Economic Cooperation and Development (OECD) which has formulated Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[22] Both legal provisions have played a key role as a framework for measures regarding the protection of the electronic personal data. They also lay down the principle that personal data have to be properly protected at all stages of processing (e.g. the stages of data collection, retention, and disclosure).

D. Personal Data Protection in Thailand

In Thailand, the right to privacy has been guaranteed by the Constitution.[23] In general, both the public and the private sectors are prohibited from disclosing personal information. According to section 5 of the Draft Personal Data Protection Act, "personal data" means "any data pertaining

[20] The Land of Hesse (1970) of Germany was originally drafted in order to tackle with this problem. Later, there are several laws which were legislated in order to cope with this matter (e.g. the law in Sweden (1973), the United States of America (1974), and France (1978)), available at http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1510&context=iclr.

[21] ETC No.108, Available at https://rm.coe.int/1680078b37

[22] C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79 Available at https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[23] Article 35 of CONSTITUTION OF THE KINGDOM OF THAILAND (2007), Available at https://www.unodc.org/tldb/pdf/Thailand_const_2007.pdf

to a person, which enables the identification of such person, whether direct or indirect". Direct data includes name and surname while indirect data are, for example, IP Address number and telephone number. Both direct and indirect data could be used in order to reach the information of the data owner.[24]

The examples of the disclosure of personal information are as follows:

1) Publishing telephone number of a person by advertising on the internet that the owner of the telephone number would like to sell goods. As a result, there are many people make phone calls on that number. This conduct causes annoyance to the owner of the telephone number.
2) A bank sells the information regarding name and address of its clients to other people by using the bank's database in order to get access to the data. The database targets a group of clients by using their personal information (e.g. age, credit limit, and payment history etc.). Then, the bank makes a label for the information buyer to use the data in order to make a sales document, which will be sent to the bank's clients.
3) A hotel records the plate numbers of its customers' cars or its guests' information according to the hotel's duty under the law. However, the hotel's staff later discloses the plate numbers or the guests' information to the outsiders.

Hence, the citizens shall retain their rights and freedom to be let alone and free from being spied or interfered by others. At present, the level and frequency of the infringement of personal information has been increasing because of the dissemination of information through social networks and the internet.[25] In order to protect privacy right of the Thai citizens more efficiently and effectively, the government has created measures by drafting and passing laws in order to tackle this problem. These laws are the Official Information Act, B.E. 2540 (1997), the Draft National Cyber Security Act, B.E. …, the Computer Crime, B.E. 2550 (2007) and its new draft legislation, and the Draft Personal Data Protection Act, B.E. …

[24] Watchara Neitivanich & Chatchai Khankwamdee, Communication and Information Technology Law, at 173 (4th ed. 2016).
[25] Rujira Bunnak, Personal Data Protection (Nov. 3, 2016), http://www.naewna.com/politic/columnist/14844

(i) The Official Information Act, B.E. 2540 (1997)

The objective of the Official Information Act[26], B.E. 2540 (1997) is to give an opportunity for the people to know the information regarding the functioning of the government organization. According to the Act, "personal information" means any information relating to all the personal particulars of a person, such as education, financial status, health record, criminal record or employment record, which contain the name of such person or contain a numeric reference, code or such other indications identifying that person as fingerprint, tape or diskette in which a person's sound is recorded, or photograph, and shall also include information relating to personal particulars of the deceased…"

State officials have to keep any personal information in secret unless a disclosure is permitted by the data owner.[27] If a state official has acted against this law by disclosing personal information, the state official will be punished under section 157 of the Thai Criminal Code[28] for his wrongful act.

(ii) The Computer Crime Act, B.E. 2550 (2007)

The Computer Crime Act[29] has laid down the principle to protect the right to privacy. It provides legal duties and responsibilities of state officials to prohibit the disclosure of personal

[26] Available at http://web.krisdika.go.th/data/outsitedata/outsite21/file/OFFICIAL_INFORMATION_ACT,_B.E._2540.pdf

[27] Section 24 of The Official Information Act, B.E. 2540 (1997) states that " a state agency shall not disclose personal information in its control to other State agencies or other persons without prior or immediate consent given in writing by the person who is the subject thereof except for the disclosure in the following circumstances…"

[28] Section 157 states that "whoever, being an official, wrongfully exercises or does not exercise any of his functions to the injury of any person, or dishonestly exercises or omits to exercise any of his functions, shall be punished with imprisonment of one to ten years or fined of two thousand to twenty thousand Baht, or both.", available at http://library.siam-legal.com/thai-law/criminal-code-malfeasance-in-office-sections-151-157/

[29] Act on Computer Crime, B.E. 2550 (2007) available at https://advox.globalvoices.org/wp-content/downloads/Act_on_Computer_Crime_2550%282007%29.pdf

information without the permission of the data subject. At present, there is a new bill of the Computer Crime Act. It is expected that the draft legislation will come into effect this year.

Duties and Responsibilities under the 2007 Act[30]

A competent official means a person appointed by a Minister for the execution of this act.[31] The competent official is responsible to comply with privacy protection pursuant to section 22 of the Act. They have no authority to disclose or deliver computer data, computer traffic data or service users' data acquired to any person.[32]

The provision stipulated that the competent official cannot apply to any act performed for the benefit of lodging a lawsuit against a person who has committed an offence or against a competent official on the grounds of his or her abuse of power or for action taken according to a Court's writ or permission. Any competent official who perform illegally must be subject to imprisonment for no longer than three years or a fine of not more than sixty thousand baht, or both.[33]

For example, a competent official displays the information of IP address of a suspect in order to make a statement. Then, a reporter checks up the IP address and finds that it belongs to a famous actor. In this situation, it can be considered that the official has acted against the provision of section 22 by disclosing personal data. In terms of liability of the official, section 23 states that any "competent official who commits an act of negligence that causes a third party to know of computer data, computer traffic data or a service user's data acquired under Section 18 must be subject to imprisonment for no more than one year or a fine of not more than twenty thousand baht, or both". Therefore, an official's negligent conduct is sufficient as a ground for liability under this act.

[30] Available at http://itserv.ait.ac.th/helpdesk/announce/cc_laws_eng.pdf

[31] Section 3 of The Computer Crime Act, B.E. 2550 (2007)

[32] Section 18 of The Computer Crime Act, B.E. 2550 (2007)

[33] Section 22 of The Computer Crime Act, B.E. 2550 (2007)

Another example is that a state official who has a duty to do traffic data replication by making a hard copy fails to destroy the printout. If a housekeeper finds the copy and brings it to a reporter who uses it to look for a suspect, the negligent conduct of the state official has revealed a secret to another person. Hence, the state official will be liable for his act.

Liability under the 2007 Act

Section 24 states that any "Whoever having gained a knowledge of the computer data, traffic data or user's information which the competent official has obtained according to Section 18, discloses the same to a third party, shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both."[34] There are two grounds of legal liabilities in this section: accessing to personal information in the computer system and eavesdropping.

Case Study on the Computer Crime Act 2007

A case on liability of a hacker

Case No. 3713/2554 can demonstrate the application of the Computer Crime Act 2007[35] by the court. The legal issues raised in this case concern illegal access to the computer system and computer data, burglary at night, and wrongful use of electronic cards of other people. The internet banking system of Siam Commercial Bank was hacked by the defendants 39 times. The defendant withdrew cash from the bank accounts of 14 bank clients for the amount of 103,050 baht (around 2,933 USD).[36] The defendant claimed that he spent the stolen money on online games.

[34] Section 24 of The Computer Crime Act, B.E. 2550 (2007)

[35] Available at http://itserv.ait.ac.th/helpdesk/announce/cc_laws_eng.pdf

[36] National Broadcasting and Telecommunication Commission, Cyber Crime (Nov. 5, 2016), http://1secure.nbtc.go.th/?p=318

The Court held that the defendant acted with malice and selfishness. His criminal conduct was a threat to the society. The defendant was found guilty and liable under the Criminal Code (sections 269/5, 269/7, 334, and 335) and the Computer Crime Act 2007 (sections 3, 5, 7, and 9). Therefore, the hacker was sentenced to 117 years imprisonment. He was also fined for the amount of 35,000 baht (around 996 USD). During the court proceeding, the defendant made a confession which was beneficial to the case. In addition, he compensated the victims for the amount of 103,050 baht. The court thereby reduced the penalty to 20 years imprisonment and a fine of 17,550 baht.

After checking the defendant's criminal record, the Court found that he had never committed any criminal offence prior to this incident. Hence, the court held that the defendant deserved to have an opportunity to reform himself. Finally, his sentence was suspended and the defendant was placed on probation for 2 years. The defendant had to report to the probation officials 8 times and do community service for 48 hours.

A case on state monitoring in Thailand

The case of Mr. Harit Mahaton is selected to demonstrate the practice of state monitoring in Thailand in relation to the application of the Computer Crime Act 2007. [37] Mr. Mahaton is a 25-year-old man who owns small local businesses (i.e. Ramen and Hainan chicken-rice restaurants) in Khon Kaen province in Thailand and Laos. Apart from his passion in doing business, he is also a writer of fiction. Mr. Mahaton has never joined any political movements or political activities. He normally uses Facebook to share innocuous information on it (e.g. his travelling, comics, cosplays etc.).

However, on April 27, 2016 Mr. Mahaton was arrested by the military officials who also rifled his house in search of evidence of Mr. Mahaton's offence. Mr. Mahaton was alleged to commit an offence under sections 116[38] (a charge of incitement) and section 112[39] (lese majesty) of the

[37]The National Human Rights Commission of Thailand, Arrested 2 Writer-Ramen Restaurant Owners to Khon Kaen Military Camp after Finding Postings Against the Order of the National Council for Peace and Order, (Apr. 27, 2016, 14:12 p.m.) (in Thai), http://www.nhrc.or.th/News/HumanrightsNews/.

[38] Section 116 states that "whoever makes an appearance to the public by words, writings or any other means which is not an act within the purpose of the Constitution or for expressing an honest opinion or criticism in order:

Criminal Code and section 14(1), 14 (2), and 14(3)[40] of the Computer Crime Act 2007. This arrest occurred after Mr. Mahoton has posted a message on his Facebook. The contents of his posting were about the authoritarian attitudes of the government and the Royal family.

On April 28, 2016, Mr. Mahaton was sent to jail and the Military Court refused to grant him bail. Mr. Mahoton's action was considered as a serious threat to the national security. He was accused of being a key administrator managing the contents of a political satire page called "Rao Ruk Pon Ake Prayoot" (i.e. we love General Prayut[41]), which used very rude and aggressive words. The military officials claimed that they had monitored Mr. Mahaton's conduct on social networks and found that there was reliable and sufficient evidence regarding Mr. Mahaton's violation of the Computer Crime Act 2007. As a result, Mr. Mahaton was imprisoned for 70 days. Finally, Mr. Mahaton was released on bail in order to fight all allegations in a lawsuit against the state.

(iii) **The Draft Personal Data Protection Act B.E. …**[42]

In the process of drafting this Bill, the drafters used the principles regarding personal data protection of the Organization for Economic Cooperation and Development (OECD) and the Directive 95/46/EC of the European Parliament as their guidelines to the processing. As for later

---

1. To bring about a change in the Laws of the Country or the Government by the use of force or violence;
2. To raise unrest and disaffection amongst the people in a manner likely to cause disturbance in the country; or
3. To cause the people to transgress the laws of the Country, shall be punished with imprisonment not exceeding seven years."

[39] Section 112 states that "whoever, defames, insults or threatens the King, the Queen, the Heir-apparent or the Regent, shall be punished with imprisonment of three to fifteen years."

[40] Section 14 states that "any person commits any offence of the following acts shall be subject to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both:

(1) that involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public;

(2) that involves import to a computer system of false computer data in a manner that is likely to damage the national security or cause a public panic;

(3) that involves import to a computer system of any computer data related with an offence against the Kingdom's security under the Criminal Code"

[41] Prayut Chan-o-cha is a retired Royal Thai Army officer who is the head of the National Council for Peace and Order (NCPO), a military junta, and concurrently serves as the Prime Minister of Thailand.

[42] Available at https://thainetizen.org/wp-content/uploads/2015/01/personal-data-protection-bill-20150106-en.pdf

drafts, a comparative study of the laws regarding personal data protection in Germany, the United Kingdom, Australia and Hong Kong was conducted in order to refine the draft.

The Bill is introduced to protect the right in "personal data." According to the Bill, a "data subject" means a person exercising the parental power who possesses the authority to act on behalf of a minor, a guardian who has the authority to act on behalf of an incapacitated person, or a curator who has the authority to act on behalf of a quasi-incompetent person. The draft legislation also provides a definition for a "personal data administrator," which is a person or juristic person who has the authority to make a decision regarding the data collection and dissemination. The draft legislation has stipulated the protection of personal data by imposing duties on the personal data controller and it also describes the rights of a data owner.[43]

Duty of a personal data administrator and the rights of a data owner

This act has imposed a duty on a personal data administrator.[44] A personal data administrator cannot collect, use, or disclose personal data without the data owner's consent given prior to or during such collection, use, or disclosure, except where there is a provision in this Act or other laws allow him or her to do so.[45] The data owner is able to withdraw consent to the collection, use, or disclosure of his or her personal information at any time. In addition, the processing of personal data must be done in accordance with the purpose that the personal data administrator has informed the data owner.[46]

Meanwhile, the personal data administrator has a duty to issue a security measure in order to prevent an unlawful act which causes loss, access, use, or disclosure of personal information without any authority.[47] The personal data administrator has to destroy the data once the period of storage has expired or the data owner has indicated his or her intention to withdraw consent.[48]

[43] Section 22 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[44] Section 31 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[45] Section 26 and 27 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[46] Section 28 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[47] Section 31(1) of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[48] Section 31(3) of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …

Moreover, according to section 31(4)[49], a personal data administrator has a duty to inform a data owner regarding the details of the information collection as well as the data owner's right and Section 23 prohibits the collection of personal data without consent from the data owner with some exceptions (e.g. where it is conducted for the benefit of research or statistics collection provided that the personal data is kept confidential.[50]

However, section 23 makes exceptions that a personal data administrator might be able to collect personal data with the data owner's permission in limited circumstances. (E.g. personal data is collected by observing a performance, sport or similar activities if the data owner voluntarily participates in that activity. In addition, the activity must be open to the public). With regards to the collection of sensitive personal data, the data collectors is prohibited to collect the data which is related to sexual behavior, criminal record, health record, origin of race, political opinion, religious belief or, etc.[51] The rational of the law is that collecting such data might cause conflicts among people in the society. Moreover, this may result in a serious damage to the data owner.

Furthermore, a personal data administrator has a duty to inform the data owner regarding the details of the personal data administrator (e.g. name, legal status of a person or a juristic person etc.), objectives of the data collection, retention period of personal data and other details as stipulated by the Personal Data Protection Committee.[52]

With regards to the rights of a data owner, they have the rights to get access to his or her personal information.[53] The data owner could ask for a copy or a certified copy of his or her personal information. In addition, the data owner has a right to know the availability, use or disclosure of his or her personal information. If the data owner finds that the information is incorrect, that person has a right to request a personal data administrator to correct the information or suppress the use or dissemination of the data.[54] In case the retention period of the

[49] "To inform the Data Owner of any incident of violation of personal data without delay and of the plan to remedy the damage caused by such violation…"
[50] Section 23 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[51] Section 25 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[52] Section 7 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[53] Section 28 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[54] Section 30 of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …

personal data has expired, a data owner could request the personal data controller to remove or destroy the data.[55]

(iv) **The Draft National Cyber Security Act, B.E. …**[56]

The purpose of the National Cyber Security Act is to support the functioning of the economy. The Act will establish an organization within the Ministry of Digital Economy and Society which deals with cyber-crime. This organization is expected to coordinate with investors and ensure the investors' confidence in the functioning of the online market. Nonetheless, there are some ambiguities in the law regarding the right of access to the information of state officials.

For example, the definition of "cyber security" provided in the draft legislation means that any measure or performance which is pursued in order to ensure the security of information and communication technology or prevent the threat to satellite communications, satellite network, telecommunications network, or other similar things are all within the authority of the state under this Act . Hence, the draft legislation provides considerable power to the state. Officials could use their power to interfere with the private sphere of the people under the guise of preventing cyber-crime and bolstering investors' confidence in online business.

In addition, section 35 of the draft legislation provides a wide-ranging power for state officials to request any public organization or person to give statement, submit a written document, or other evidence for the sake of an investigation or an official's performance under this Act. Moreover, a state official may send a letter requesting any public or private organizations to act for the benefit of the functioning of the "National Cybersecurity Committee" (NCSC), which will be created under this Act.[57] Hence, an officer who receives an order from the secretary of the NCSC is allowed to inspect or get access to the information that people communicate via mail, telephone, fax, computer, equipment or device for communication, electronic media, or other information technology resources.

[55] Section 31(3) of Memorandum of Principles and Rationale of [Draft] Personal Data Protection Act B.E. …
[56] Available at https://thainetizen.org/wp-content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf
[57] Section 35 of Memorandum of Principle and Rationale of [Draft] National Cybersecurity Act B.E. …

Part II: Liability for Intrusion of Privacy Right

It is essential for all citizens to have a protecting measure in order to ensure their privacy right. For instance, personal information has to be protected from the intrusion by others and the unauthorized disclosure to the public. There are some protections which the technology can provide (e.g. using password). However, this cannot guarantee that the data will be 100% safe as the information might be hacked. Hackers can destroy data protection system and use or release the information to a third party in order to cause damage to the data owner or other people. The disclosure of information without a data owner's permission would constitute an infringement upon his or her rights and liberties.

As a result, there is a need for the law to prevent violations of those rights and liberties. There are at least four Acts, as mentioned earlier, which deal with the invasion of privacy rights. However, if there is a case that the liability of a privacy intruder could not be found in those Acts, the Civil and Commercial Code, and the Criminal Code of Thailand will be applied in order to fill in the gap of the law. This part of the Paper will describe those liabilities by categorizing them into three groups: civil, criminal, and administrative liabilities.

A. Civil Liability

Civil liability regarding privacy right violation is not stipulated in any piece of legislation specifically. The only piece of legislation which mentions civil liability is the Draft Personal Data Protection Act.[58] However, it has yet come into force. According to section 42 of the Bill, a personal data administrator, who causes damage to a data owner by acting intentionally or negligently in the operation of the personal data, has to compensate for such damage to the data owner. However, there are some exceptions in the case that the personal data administrator could prove that the damage was caused by a force majeure (act of god), and act or forbearance of the owner of the personal information.[59] Other exceptions are that the personal data administrator's

[58] *Supra* note 42.
[59] Section 42 of the Draft Personal Data Protection Act.

action is taken in compliance with an order of the government or a government official, or the practice on personal data protection issued by the Personal Data Protection Committee.

With regards to other civil liabilities which are not covered by the Personal Data Protection Act, sections 420 and 438 of the Civil and Commercial Code could be applied in the case of privacy right violation. Section 420 states that "a person who, willfully or negligently, unlawfully injures the life, body, health, liberty, property or any right of another person, is said to commit a wrongful act and is bound to make compensation" for his or her act. Meanwhile, section 438 stipulates that the Court shall determine the compensation which includes restitution of the property and its value as well as the damages for any injury caused by the wrongful act.

B. Criminal Liability

Criminal liability is provided, in part, by the Computer Crime Act 2007.[60] First, the 2007 Act criminalizes an act of accessing another person's computer system despite the fact that there is no disclosure of the information to the public (sections 5 and section 6). Second, sections 7 and section 8 make it a criminal offence for an illegal access to the computer data without any permission or authority. This offense includes an information interception of the transmission system. The offense is under the umbrella of the violation of privacy right in information and the computer system.

Third, sections 9 and section 10 stipulate the liability for any performance which changes or destroys computer data, interferes, disrupts, or delays the computer systems of other.[61] The penalty for so doing would be more severe if there is damage to the public or a tendency that there might be damage to the national security or public interest (section 12).

Fourth, section 11 provides liability for an act of sending computer data or electronic mail.[62] As a result of this act, there is an interruption on the normal operation of the computer system of others. Such act will constitute an offence if the source of such data is concealed or disguised.

[60] *Supra* note 29.
[61] Section 9 and 10 of the Computer-Related Crime Act B.E. 2550 (2007)
[62] Section 11 of the Computer-Related Crime Act B.E. 2550 (2007)

The offence under section 11 is criminalized because it is an interference in the privacy right of other people.

Finally, section 22 contains the liability regarding the information disclosure or delivery to any person by a competent official who holds computer data, traffic data, or service users' data.[63] However, section 22 provides exceptions to liability in the case where an action is performed for the benefit of lodging a lawsuit against a person who has committed an offense under this act or a competent official on the grounds of their abuse of authority, or for action taken according to a court's instruction or permission.

C. **Administrative Liability**

The Official Information Act, B.E. 2540[64] and the Personal Data Protection Bill[65] stipulate some administrative liabilities for the infringement of personal data.

(i) The Official Information Act, B.E. 2540

Section 40 provides liability in the case where a person fails to comply with the order of the Official Information Board according to section 32, which authorizes the Board to summon any person to give statements or furnish any evidences or documents for consideration. Another administrative liability which could arise under this Act is stated in section 41. According to section 41, there will be a liability in the case that a person fails to comply with the restriction or condition ordered by a state official who acts in accordance with the Act. Nevertheless, it should be noted that the liabilities provided by the Act are only for failure to comply with the order of public officials. The Act provide no the privacy right of action.

(ii) The Personal Data Protection Bill

There is an administrative liability under section 46 of the Bill. The purpose of section 46 is to promote the efficiency in the justice system. According to section 46, any person who fails to comply with the order of the Expert Committee, breach a summons under section 40, or refuse to

---

[63] Section 22 of the Computer-Related Crime Act B.E. 2550 (2007)
[64] Available at http://web.krisdika.go.th/data/outsitedata/outsite21/file/OFFICIAL_INFORMATION_ACT,_B.E._2540.pdf

[65] *Supra* note 42.

facilitate the functioning of the competent officials under section 41 (3)[66] shall be fined for no more than 100,000 baht.

Part III: The Analysis of the Draft Legislations

A. The Draft National Cyber Security Act, B.E….[67]

The inauguration of the current Thai government's policy of "Digital Economy" leads to the creation of "Digital Economy Law," which is comprised of many Acts. The National Cyber Security Act, B.E…. is one of the pieces of legislation in the digital economy law. The purpose and the content of the Act are to facilitate the use of state power in order to prevent cybersecurity threat as well as economic, social and military security which is part of national security.[68] However, the draft legislation has raised concerns among Thai people regarding whether or not the State has gained too much power as amount to an infringement of rights and liberties of the people. Hence, the authors will analyze the draft legislation in terms of benefits and losses to Thailand that might occur as a result of having this piece of legislation.

Does Thailand need to have a National Cyber Security Act?

Many countries have enacted national cybersecurity legislation in response to threats of cyber attacks, which occurs from time to time (e.g. the United States, the European Union, China and North Korea). For example, there was a hack of personal information of millions of government employees of the US Office of Personal Management in 2014.[69] In addition, Chinese hackers have been spying on governments and businesses in the members states of the Association of

[66] Section 41 (3) authorizes a competent official to enter into a place of a personal data administrator and any person involving in the illegal conduct under this Act in order to inspect, collect or seize document and evidence of the illegal act. The official can do so if it is necessary for protecting the data owner's interest or public interest.
[67] *Supra* note 56.
[68] Memorandum of the principles and rationales of the Draft National Cyber Security Act, available in Thai at https://ictlawcenter.etda.or.th/de_laws/download_file/1_Cabinet_Draft-de_laws_cyber-security-protection-act.pdf.
[69] Brian Barret, Hack Brief: Hacker Leaks the Info of Thousands of FBI and DHS Employees, Wired (Aug. 2, 2016: 3:33 p.m.), https://www.wired.com/2016/02/hack-brief-fbi-and-dhs-are-targets-in-employee-info-hack/.

South East Asian Nations (ASEAN) and India for a decade.[70] Consequently, the costs for cyber-defense around the world have been increased. In Asia-Pacific countries, there was an increase of the costs of 9.8% in 2015 or 17,900 million dollars. There will be an increase of the cyber-defence costs of 45% from that of the year 2014 (around 23,800 million dollars) by 2018.[71]

Thailand ranked the 33th out of 250 countries around the world for the most frequently cyber-attacked countries. The unavailability of a law for which the state could use to protect its citizens from cyber threat would be alarming. Therefore, the government of General Prayut Chan-o-cha has made an integrated policy to deal with both cyber security and economic growth.[72] The National Cyber Security Act would help to implement this policy by providing security to the network system and the Internet. Apart from passing the Act, there would be a need to create a holistic system in which the state, the private sector, and the civil society have a role to play in regulating the Internet. This could be done in the form of statutory regulation that the state promulgates rules and laws in order to regulate the society. In addition, the state could create a system of co-regulation that the state, the private sector and the civil society help regulate the Internet. For example, the private sector and the civil society might create a network which they share and report the information about digital crimes to the state.

However, there are some concerns among Thai people regarding the danger of passing this draft legislation. First, it is arguable that the issue of national security is different from that of cybersecurity. Hence, the claim that the government needs to protect cybersecurity as part of the protecting national security is arguably weak. If this is the case, the government needs to explain why cybersecurity is so important as to give them the right to have such a piece of legislation.

Second, the structure of the National Cybersecurity Committee (NCSC)[73] which possesses a wide-ranging power in regulating the use of the Internet has raised a concern that the Committee might interfere with the protection of privacy right under other related Acts (e.g. the Personal

[70]Jeremy Wagstaff, Chinese Hackers Target Southeast Asia, India, Researchers Say, Reuters (Apr. 13, 2015: 5:00 a.m.). http://www.reuters.com/article/us-cybersecurity-fireeye-report-idUSKBN0N40AD20150413.
[71]Asia Spent Big on Preventing Cyber-Attacks, Bangkokbiznews.com (Apr. 5, 2015) (in Thai), http://www.bangkokbiznews.com/news/detail/642706.
[72] Sarawut Pitiyasuk, The Analysis of the Draft National Cyber Security Act, B.E. …: A Comparative Study of Strategies and European Union Network and Information Security Directive, Sukothai Thammathirat Law Journal, 27 (2) April 2016, p. 1 (*in Thai)*
[73] Section 6 of the National Cybersecurity Act, B.E, ,,,

Data Protection Act).[74] This is especially the case when considering the fact that one of the NCSC ex officio members is the Permanent Secretary of the Ministry of Digital Economy and Society. This person is also an ex officio member of the Personal Data Protection Committee created under the Personal Data Protection Act. Hence, there might be a situation where in order to achieve the goal of the NCSC, the Permanent Secretary of the Ministry of Digital Economy and Society might choose to sacrifice the protection of privacy right.

Also, the draft legislation has given significant power to state agencies in getting access to personal data of the citizens. In theory, this authorized power under the draft legislation might breach the underlying principles in public law - the principles of necessity and proportionality.[75] In the Thai legal system when the state passes an Act that interferes with rights and liberties of the people, the state has to consider whether the benefits of so doing outweigh the losses to the people.[76] In order to balance the benefits and losses, the principles of necessity and proportionality must be taken into account before reaching the conclusion of whether or not the law is appropriate.[77]

With regards to the abovementioned arguments, the authors are of the opinion that, first, there is a strong connection between the issue of national security and that of cybersecurity. The policy of the current government is formulated to switch itself to a digital government. Therefore, many of the government's tasks have to be done via digital means. A cyber-attack could therefore destroy a smooth functioning of the government of the day and future governments.

Second, according to the section 14 of the draft legislation, the National Cybersecurity Committee is a public organization which is a juristic person. [78] Therefore, if the NCSC's action or order is illegal or ultra vires, the effected citizen could pursue his or her case in the

[74] The Personal Data Protection Committee is established under section 7 of the Draft Personal Data Protection Act, B.E. …

[75] Section 26 of the Thai Constitution B.E.2560.

[76] Section 26 and 32 of the Thai Constitution B.E, 2560 states the principles of proportionality and necessity. In the Thai Constitutional Court. There are also judicial decisions regarding this matter.

[77] Bancherd Singhaneti, The Fundamental Principles of Rights, Liberties and Human Rights, Winyuchon: Bangkok (2012,4th edition)

[78]Section 14 of the Draft National Cybersecurity Act B.E. … states that the "Office of the National Cybersecurity Committee shall be set up as a State agency having a juristic person, not being a State division or a State enterprise." Available at https://thainetizen.org/wp-content/uploads/2015/03/cybersecurity-bill-20150106-en.pdf

administrative court. In addition, if an officer, who acts under the order of the NCSC, conducts a criminal offence, the officer will be punished according to Thai criminal law.[79]

Last, the theoretical concern about the breach of the principles of necessity and proportionality will be discussed. With regards to the principle of necessity, in the Thai legal system a legal measure must be limited to what is necessary to achieve the objectives of the law.[80] The relative effectiveness of alternative measures must be taken into account. Then, the measure which generates the most minimal infringement on rights and liberties of the people will be selected. The alternative measures must also be considered in the light of the current stage of technological development. At present, there are many measures which could help prevent the threat of cyber-security. For example, important websites can be protected from being attacked by using Web Application Firewall and DDoS Protection. However, these measures do not guarantee that websites will be 100% safe.

Besides, the National Cybersecurity Act is necessary and important because terrorism takes various forms nowadays. The state would need to respond and act promptly in order to cease them. However, the use of many Acts of Parliament to chase all situations of terrorisms might be clumsy and inefficient.[81] The slow process of state action would not be in the best interest of the people.

Concerning the principle of proportionality, in the Thai legal system the narrow meaning of this principle means a legal measure, which infringes upon the rights and liberties of the people, must be appropriate and necessary.[82] Moreover, the values of the legal measure must outweigh the losses which might occur as a result of having it. If the benefits of the measure are less than the

[79] According to the Thai Criminal Code, no public official could deny liability in the case of his or her misconduct.
[80] There are four elements when considering this principle. The Thai Constitutional Court has laid down these four elements which are:

1. The objective must be definite.
2. The measure must be able to achieve the objective
3. The measure must infringe on rights and liberties of the people in the least detrimental way.

[81] At present, there are some Emergency decrees which deal with the issue of terrorism. For example, the Emergency Decree Amending the Criminal Code, B.E. 2546 has added terrorism as one of the ground for criminal acts in sections 135/1-135/4. In addition, there is an Emergency Decree amending the Money Laundering Act (B.E. 2542), B.E. 2546 which has added terrorism to the ground for criminal acts according to the Money Laundering Act.
[82] Worrapot Wisarutpit, Fundamental Principles of Administrative Law. Law Faculty of Thammasat University Press (1995), p.48.

losses that people will have to sacrifice, the state must not promulgate that measure even though it is necessary and appropriate.[83]

In the context of the National Cybersecurity Act, there is value for the public interest in reducing cyber threats through legislation, which could resolve this problem systematically and uniformly. The losses that the people might have to sacrifice are the infringement upon their rights and liberties. For example, according to section 35(3) an officer who receives an order from the secretary of the NCSC is allowed to inspect or get access to the information that people communicate via mail, telephone, fax, computer, equipment or device for communication, electronic media or other information technology resources.[84] This is despite the fact that no court warrant is required to do so. However, it must be conducted according to the criteria and rules stipulated by the cabinet for the sake of maintaining cybersecurity.

In addition, section 35 (2) authorizes the NCSC to request private organizations to act for the benefits of the functioning of the NCSC. Moreover, where it is necessary to maintain cyber-security which might affect security of finance, commerce, or national security, the NCSC could order private organizations to either act or not to act (section 34). This power of the state agencies might interfere with freedom of foreign or international corporations which operate their business in Thailand.

However, when balancing the values of public interest against the losses of private interest, the authors have reached a conclusion that this draft legislation is proportional. National security is crucially important. In addition, the use of state power in accessing to the information is limited by legal protection of rights and liberties of the people. These limitations are, for example, section 25 (3) of the draft Constitution of Thailand 2016 which provides that a person could "invoke the provisions of the Constitution to exercise his or her judicial right or to defend himself or herself in court" when his or her rights or liberties are violated. [85]

[83] *Id.*
[84] Section 35 (3) of the Draft National Cybersecurity Act.
[85] "A person whose rights and liberties recognized by the Constitution are violated may invoke the provisions of the Constitution to exercise his or her judicial right or to defend himself or herself in court". The Draft Constitution of the Kingdom of Thailand 2016. *available at* http://www.constitutionnet.org/files/thailand-draft-constitution_englishtranslation_june_2016.pdf

Moreover, there is no provision in this draft legislation that prohibits the court from reviewing the use of state power. Despite the fact that this draft legislation is a national security law, there is no provision that expressly excludes liability of the officials. This is different from other national security laws that have an exemption clause of state liability (e.g. the Martial Law (1914)[86] and the Administration of the Country in a State of Emergency Decree (2005).[87] Therefore, in the case that there is any misuse of power by a state authority, a person could sue the public authority in the Administrative Court.

B. The Computer Crime Act (No.2) B.E. 2560 (A.D. 2017)[88]

The 2017 Act is one of the digital economy laws that is heavily criticized for its infringement upon freedom of expression in the digital world. In addition, there were many enforcement problems resulting from the use of the previous Computer Crime Act 2007.[89] For example, section 14 (1) of the 2007 Act was frequently used to pursue defamation litigations in the court. This is despite the fact that the objective of the Act was to deal with problems of defraud and online phishing.[90] The authors will analyze the pros and cons of this Act in terms of values of public interest when compared with the losses to the private sector in order to find the conclusion of whether or not this piece of legislation is appropriate.

The values of public interest provided by the Computer Crime Act 2017.

[86] Section 16 states that "No compensation or indemnity for any damage which may result from the exercise of powers of the military authority as prescribed in sections 8 to section 15 may be claimed from the military authority by any person or company, because all powers are exercised by the military authority in the execution of this Martial Law with a view to preserving, by military force, the prosperity, freedom, peace and internal or external security for the King, the Nation and the religion." *available at* http://www.thailawforum.com/laws/Martial%20Law.pdf.
[87]http://www.asianlii.org/th/legis/consol_act/edopaies2005582/
[88] The Act was published in the Royal Gazette on January 24, 2017. It came into effect in May 24, 2017.
[89] For example, the law was used to pursue lese-majeste cases. For more information, please see Thailand: Cybercrime Acts vs. the Right to Freedom of Expression available at https://thainetizen.org/wp-content/uploads/2011/06/thailand-cybercrime-foe-20110602.pdf
[90]NLA defends computer crime review, *The Nation* (November 24, 2016) available at http://www.nationmultimedia.com/news/national/30300706

First, the 2017 Act will help solve the problem of interpretation by making the application of the law more consistent with its objective. Section 8 of the 2017 Act has amended section 14 (1) of the Computer Crime Act 2007. Previously, section 14 (1) was interpreted by judges to include defamatory postings and internet slander.[91] Therefore, the current Act is carefully written to prevent misinterpretation by using phrases which are more precise than those of the previous legislation. For example, section 8 states clearly that an offence under this law must not be an illegal act according to the criminal law.[92] Besides, the Computer Crime Act 2007 was previously used to pursue a case that caused damage to an individual person. The new Act indicates that the damage must occur to the public at large.[93]

Second, the 2017 Act adds new grounds on which to claim damages. Previously, section 14 (2) of the Computer Crime Act 2007 provided that, apart from causing panic to the public, an act which is likely to damage national security was the only ground of action under this subsection. The 2017 Act includes damage to the maintenance of national security, public safety, national economic security, and public infrastructure serving public interest as new grounds of action.[94]

Third, section 13 of the 2017 Act consolidates the laws regarding digital crimes which were previously dispersed in many pieces of legislation into this single Act by amending section 18 (2) and section 19 of the 2007 Act. This will be convenient for the law enforcers and users that they no longer need to search for the law in many pieces of legislation.

The benefits for the private sector

The 2017 Act benefits the private sector in many aspects. First, it adds a safe harbor for the Internet Service Providers (ISP). Sections 14 and section 15 of the Computer Crime Act 2007

[91] The Truth about Slander and Liber Laws in Thailand. Available at http://silklegal.com/the-truth-about-slander-and-libel-laws-in-thailand/

[92] Section 326 of the Thai Criminal Code states that "whoever, imputes anything to the other person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to be hated or scorned, is said to commit defamation, and shall be punished with imprisonment not exceeding one year or fined not exceeding twenty thousand Baht, or both." Available at http://library.siam-legal.com/thai-law/criminal-code-defamation-sections-326-333/

[93] Section 8 of the Computer Crime Act (No.2) B.E. 2560 (A.D.2017).

[94] Section 8 of the Computer Crime Act (No.2) B.E. 2560 (A.D.2017).

created a risk for the service providers that they might break the law if they put into a computer system forged computer data, partially or entirely, or false computer data. In contrast, section 9 of the 2017 Act has amended section 15 (3) of the 2007 Act. It stipulates that the service providers who are able to prove that they have complied with procedural rules issued by the Minister shall be exempted from penalty.[95] The details of the Ministerial procedural rules are made according to section 9 of the 2017 Act that has amended section 15 (2) of the 2007 Act. According to section 9 of the 2017 Act, the Minister shall issue procedural rules indicating steps for notice, a request for suppression of the dissemination of data, and the removal of data from the computer system.

Moreover, section 14 of the 2017 Act that has amended section 20 of the previous piece of legislation gives power to the Minister to appoint one or more than one Computer Data Screening Committee.[96] Each committee comprises nine members. Three of them must be representatives from the private sector who are specialized in human rights, information technology, or other related fields. When considering the structure of the Computer Data Screening Committee, there is an improvement in terms of protecting privacy right and human rights from previous drafts. In the previous draft legislations, only 2 out of 5 committee members must be representatives of the relevant private sector. Besides, those representatives might not necessarily be human rights specialists.

Furthermore, section 14 of the 2017 Act that has amended section 20 of the 2007 Act makes the court play an important role by reviewing the use of state power. The court can either issue a writ for a competent official or instruct the service provider to suppress the dissemination or remove the computer data from the computer system. In other words, this section provides another protection of rights and liberties for the private sector apart from the Computer Data Screening Committee. In order to control the use of state power, the court could summon the service providers to come and give them an opportunity to argue for their case before deciding to issue a court order.

[95] Available in Thai at https://ictlawcenter.etda.or.th/files/law/file/80/59100b296f08176ad3bd2c1615489253.pdf
[96] Available in Thai at https://ictlawcenter.etda.or.th/files/law/file/80/59100b296f08176ad3bd2c1615489253.pdf

The losses to the private sector

The 2017 Act has improved the protection of rights and liberties of the people in many aspects from the previous Act. However, the private sector, especially the ISP, still has to take very careful steps in complying with the law. First, mental element (mens rea) of the service provider is still arguably vague. According to the Computer Crime Act 2007, the service provider must "intentionally support or consent" to the commission of an offence.[97] However, "consent" is difficult to prove. There is no firm criterion as to what amounts to "consent."[98] The problem of this unclear term is exacerbated by the fact that the 2017 Act has changed the mens rea of the service provider to "cooperate, consent or acquiesce" to the commission of an offence. The new Act provides neither the definition of "consent" nor that of "acquiesce". Therefore, these two terms will create uncertainty for the service provider in complying with the law. As a result of this risk, some ISPs might decide not to operate in Thailand since there is no clear provision which will immune them from liability.

Second, section 14 of the 2017 Act that has amended section 20 of the 2007 Act, authorizes the competent official, with the recommendation of the Minister, to file a petition with evidence to the court.[99] Then, the court could issue a writ to suppress the dissemination or to remove such computer data from the computer system. In other words, the court is the reviewer of the use of state power by the official. However, the computer data, according to section 14 of the 2017 Act that has amended section 20 of the 2007 Act needs not be illegal according to any other law. It will be an offence under this section if the computer data is deemed to be a breach to the "public order or moral high ground of the people."[100] Nevertheless, "public order or moral high ground of the people" is a vague legal terminology, as it depends largely on the judgment of the court in each particular case. Hence, the citizens will find it difficult to predict whether or not their behavior will break the law. In addition, the service providers would need to increase their level of care in operating. They might remove any computer data which could create a risk of breach

[97] Section 15 of the Computer Crime Act 2007.
[98] There is an explanation for the meaning of "consent" that it means a person must know that there was a criminal offence according to section 14 (e.g. a notice that the computer data is illegal has been sent to the service provider but it still allows the data to be disseminated in the computer system).
[99] Available in Thai at https://ictlawcenter.etda.or.th/files/law/file/80/59100b296f08176ad3bd2c1615489253.pdf

[100] Section 14 of the Computer Crime Act 2017.

of the "public order or moral high ground of the people." Consequently, this would increase operating costs for the ISPs in monitoring content of the computer data.

Third, according to section 17 of the 2017 Act that has amended section 26 of the 2007 Act, a service provider is responsible for retaining computer traffic data for at least 90 days, which is a longer period than what was demanded in the 2007 Act. The 90-day retention period starts from the date on which the data is entered into the computer system.[101] If necessary, a competent official may instruct the service provider to retain such computer traffic data for longer than 90 days but not exceeding 2 years on a particular occasion. This duty imposed on the service providers could be financially burdensome.

Finally, complying with an order of the competent official in suppressing the dissemination or removing the computer data could be onerous. For example, THNIC, a Thai domain name registrar, may be instructed by a competent official to open up "http". In opening up the code, THNIC would need to open up every single dataset including personal data of the ISP owner and the data of trade secrets. This could make THNIC liable according to the draft legislation if there is no other provision which exempts a data holder from liability.

In sum, when balancing both the values of public interest and the losses to the private sector, the authors are of the view that the former would be less than the latter. We recommend some changes to the law in order to strike the right balance between the benefits to the state and the losses to the private sector. First, the Act should provide clear definitions for vague terms which are crucially important to a service provider's liability (e.g. "consent" and "acquiesce"). Second, there should be a provision which exempts a data holder from liability resulting from its compliance with the official's order without the fault on the part of the former.

C. The Draft Personal Data Protection Act, B.E. …[102]

The draft legislation is a response to the problem of infringement upon personal data which is increasingly worrying in Thailand. In addition, it aims to fill in the gap of the law, since there is

[101] Section 17 of the Computer Crime Act 2017.
[102] Available in Thai at https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-data-privacy-act

no legislation crafted to specifically provide protection of personal data. At present, there are many laws that are related to the use of personal data (e.g. the Official Information Act 1997[103], the Telecommunications Business Operation Act 2001[104] and the Credit Information Business Act 2002[105]). Nevertheless, the use of state power to infringe upon privacy rights as stipulated in the draft legislation has been heavily criticized by the public. Therefore, the authors will analyze the advantages and disadvantages of having this draft legislation by comparing the benefit for the public and the private sectors with the losses that the private sector and the people would suffer.

The benefit for the public and private sectors

The draft legislation could help promote and facilitate commerce. For example, the European Union (EU) has General Data Protection Regulation 2016 (GDPR) which provides a set of rules with high level of protection of personal data.[106] Trading partners of the EU must have equivalent standard of protection of personal data for there to be exchanges of data between these countries and the EU Member States. If Thailand has a high level of protection of personal data by stipulating regulation in the Personal Data Protection Act, this would clearly benefit commerce between Thailand and other countries.

The losses that the private sector and the people might suffer

The issue of consent

Consent is central to the concept of privacy rights. The right to privacy entails that a person should have control over his or her personal information. There would be an infringement of privacy right if there is an intrusion of personal affairs without that person's consent. The draft

[103] Available at http://www.asianlii.org/th/legis/consol_act/oia1997197/
[104] Available at http://muit.mahidol.ac.th/it_statute/05-2_telecommunications_statute2554_en.pdf
[105] Available at https://www.ncb.co.th/PDF/ACT/crb_act_e01.pdf
[106] The GDPR imposes obligations on both the Member States and their trading partners by creating a "level playing field in that companies based outside the European Union will have to apply the same rules as European companies" This is the case if the former are offering goods and services or monitoring the behavior of individuals in the EU. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European Data Economy"*, COM (2017) 09 final (Jan. 10, 2017). *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN.

legislation has taken into account the importance of consent by stipulating that the owner of personal data must give consent to the processing of information which includes collecting, using and disclosing data.

However, there are some concerns regarding section 17 of the draft legislation which provides an exception for the requirement of consent.[107] Section 17 stipulates that the owner of personal data must have given consent to the personal data administrator except where "a provision in this Act or other law stipulates that no consent is required."[108] This means that in many cases there will be a collection, use and disclosure of personal information without prior knowledge or consent of the data subject.

In addition, the draft legislation does not provide any definition of "consent" which is fundamental for data protection. This would result in legal uncertainty as the court will have to make a decision based on facts of each particular case regarding the issue of consent. This is different from the law of other countries. For example, Korea and the European Union have regulation on personal data that a data subject must freely give an explicit consent. In addition, a data subject must fully aware that he or she is consenting.[109]

Moreover, some academics in Thailand have argued that the requirement of "consent" in the draft legislation, which aims to safeguard privacy right of the people, does not come from the demand of the civil society. Thai people still lacks consciousness regarding privacy rights. In other words, the law merely imposes a top-down protection on the people. Therefore, the legislation might lack supports from the citizens as they do not feel that the law belongs to them.

With regards to the issue of consent, the authors are of the view that it is a core element of the protection of privacy rights. Hence, there should be a definition of consent stipulated in the legislation. This would provide clearer guidance to both law enforcers and Thai citizens. Besides, although the Thai people still do not have enough consciousness regarding privacy rights, the law might be able to create that awareness among the people. If the law could increase people's

[107] Section 17 of the Draft Personal Data Protection Act, B.E. …
[108] *Id*.
[109] *Opinion of the Working Party on the Definition of Consent*, at 11, Opinion 15/2011 (Jul. 31, 2011). *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

consciousness of privacy rights, this consciousness might later become a social norm in the society that people will pay serious attention to the protection of their personal information.

The issue of the infringement of privacy right by the state

The draft legislation creates the Personal Data Protection Committee which consists of both ex officio and qualified members.[110] The ex officio members are, for example, the Permanent Secretary of the Office of the Prime Minister and the Permanent Secretary of the Ministry of Digital Economy and Society.[111] Meanwhile, the qualified members are appointed by the Prime Minister from relevant and useful fields for the protection of personal data (e.g. representatives from the Thai Chamber of Commerce and the Consumer Protection Committee).[112] The Personal Data Protection Committee is given large power under this draft legislation. It can formulate policies, create measures, and issue guidelines for the protection of personal data in accordance with the Personal Data Protection Act.[113]

However, committee membership is part-time and the committee members have to fulfill other functions of their full-time and part-time roles. This raises a question regarding the independence of the Committee. For instance, the Permanent Secretary of the Ministry of Digital Economy and Society is also an ex officio member of the National Cybersecurity Committee. There might be conflicts in achieving the objectives of these two committees. One of the main objectives of the National Cybersecurity Committee is the protection of national security while that of the Personal Data Protection Committee is the protection of privacy right.

Besides, the Personal Data Protection Committee is comprised of committee members who have to perform their duties according to the policy of the government (e.g. the Permanent Secretary of the Ministry of Digital Economy and Society). Furthermore, the qualified committee members are appointed by the Prime Minister. Therefore, if the government would like to exercise state

[110] Section 7 of the Draft Personal Data Protection Act, B.E. …
[111] Section 7(2) of the Draft Personal Data Protection Act, B.E. …
[112] Section 7(3) of the Draft Personal Data Protection Act, B.E. …
[113] Section 13 of the Draft Personal Data Protection Act, B.E. …

power in order to control the civil society, the Personal Data Protection Committee might lack independence in their functioning.

With regards to the concern of the exercise of state power to infringe on privacy right, the authors are of the view that the independence of the Personal Data Protection Committee is crucial to this issue. Hence, the ex officio committee members of the Personal Data Protection Committee should not hold a post in any other committee of which its functions may be in conflict with those of the Personal Data Protection Committee.

Conclusion

The right to privacy is fundamentally important for human beings to live their lives happily in the society. The concept of a right to privacy means that a person should not infringe upon the private sphere of others. However, it is not an absolute right. The right to privacy has to be balanced against other competing values of society. In Thailand, people have increasingly paid attention to the importance of the right to privacy due to rapid development of the technology and the internet. In addition, the government of the day has introduced several bills which will deal with the issues relating to privacy rights (e.g. personal data protection). Nevertheless, the authors have found that these pieces of legislation still need to be improved in order to strike the right balance between competing rights and values of the state, the civil society, and the people.