of this unclear term is exacerbated by the fact that the draft legislation has changed the mens rea of the service provider to "cooperate, consent or acquiesce" to the commission of an offence. The draft legislation 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 which 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.[60] 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 which 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." [61] 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 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 which 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

---

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

[61] Section 14 of the Computer Crime Act 2017 which has amended Section 20 of the Compuer Crime Act 2007.

is entered into the computer system.[62] 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.

Lastly, 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. ... [63]

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 no legislation crafted to specifically provide protection of personal data. At present, there are many Acts which are related to the use of personal data (e.g. the Official Information Act 1997 [64], the Telecommunications

[62] Section 17 of the Computer Crime Act 2017 has amended Section 26 of the Computer Crime Act 2007.

[63] Available in Thai at https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-data-privacy-act

[64] Available at http://www.asianlii.org/th/legis/consol_act/oia1997197/

Business Operation Act 2001 [65] and the Credit Information Business Act 2002 [66]). 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 benefits for the public and the private sectors with the losses that the private sector and the people would suffer.

The benefits for the public and private sectors

The draft legislation could promote and facilitate commerce. For example, the European Union (EU) has the General Data Protection Regulation 2016 (GDPR) which provides a set of rules with high level of protection of personal data.[67] 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.

---

[65] Avaialbe at http://muit.mahidol.ac.th/it_statute/05-2_telecommunications_statute2554_en.pdf

[66] Available at https://www.ncb.co.th/PDF/ACT/crb_act_e01.pdf

[67] 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

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 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.[68] 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.[69] 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.[70]

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

---

[68] Section 17 of the Draft Personal Data Protection Act, B.E. ...

[69] Section 17 of the Draft Personal Data Protection Act, B.E. ...

[70] *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 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 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.[71] 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.[72] 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).[73] 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.[74]

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

[71] Section 7 of the Draft Personal Data Protection Act, B.E. ...

[72] Section 7(2) of the Draft Personal Data Protection Act, B.E. ...

[73] Section 7(3) of the Draft Personal Data Protection Act, B.E. ...

[74] Section 13 of the Draft Personal Data Protection Act, B.E. ...

ex officio member of the National Cyber Security Committee. There might be conflicts in achieving the objectives of these two committees. One of the main objectives of the National Cyber Security 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 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 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 current government 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.