LEGAL MEASURES FOR PROTECTING THE RIGHT TO PRIVACY IN CASE OF SHARING PERSONAL DATA VIA ONLINE COMMUNICATION

มาตรการทางกฎหมายในการคุ้มครองสิทธิส่วนบุคคลกรณีการเผยแพร่ข้อมูลส่วนบุคคลในบริบทของการสื่อสารข้อมูลออนไลน์

Kanathip Thongraweewong *

Abstract

The users of internet and online communication such as Social Network Websites and Chat applications on mobile phone, deliberately or inadvertently share data in every aspect of life. The data shared include images, telephone numbers, mailing addresses, workplaces, etc. which are considered “personal data” of the individuals. Not only personal information of users of online communication, but also that of non-users’ has been exposed online without their consent. This research has classified the sharing of personal data online into two main categories. First is the sharing of one’s own data which is associated with “self disclosure” behavior that becomes a popular trend online. Second is the sharing of others’ personal data without consent which affects the right to privacy of the data owners. Such right is regarded as a fundamental or human right. Thus, this research aims to study the application of laws relating to data protection in the context of personal data sharing online. The results indicated that, by using qualitative method and comparative analysis of Thai laws with related foreign laws, there were no specific laws in the recent Thai legal system that protected the privacy and personal data. Although there are currently various laws which can be applied to protect the right of person whose personal data have been shared online, this research indicated that the problems of content, element, and scope of such laws made them inappropriate and insufficient to protect personal data from being shared online. Consequently, the amendment of laws is proposed to mitigate the negative impact of such sharing as well as to protect the right to privacy appropriately.

Keywords : Right to privacy, Data protection, Sharing personal data online

* Associate Professor of law, Dean of Faculty of law, Saint John’s University,
e-mail : kanathip@yahoo.com

บทคัดย่อ

ผู้ใช้งานการสื่อสารข้อมูลออนไลน์ รวมถึงการสื่อสารข้อมูลทางอินเทอร์เน็ต เว็บไซต์ เครือข่ายสังคมโปรแกรมประยุกต์เพื่อการสนทนาทางโทรศัพท์เคลื่อนที่ ได้มีการเผยแพร่ข้อมูลเกี่ยวข้องกับมิติต่าง ๆ ในชีวิตของตน ข้อมูลที่ถูกเผยแพร่นั้นรวมถึง ภาพถ่าย หมายเลขโทรศัพท์ ที่อยู่อิเล็กทรอนิกส์ สถานที่ทำงาน เป็นต้น ซึ่งข้อมูลเหล่านี้จัดเป็น ข้อมูลส่วนบุคคล นอกจากการเผยแพร่ข้อมูลส่วนบุคคลดังกล่าวที่กระทำขึ้นโดยผู้ใช้งานการสื่อสารออนไลน์ดังกล่าวแล้ว ผู้ที่มิได้เป็นผู้ใช้งานการสื่อสารออนไลน์ก็อาจได้รับผลกระทบจากการถูกนำข้อมูลไปเผยแพร่ในการสื่อสารออนไลน์ด้วย งานวิจัยนี้ได้จำแนกการเผยแพร่ข้อมูลส่วนบุคคลทางการสื่อสารออกเป็นสองกรณีคือ กรณีแรก การสื่อสารข้อมูลส่วนบุคคลของตนเอง ซึ่งอยู่บนพื้นฐานพฤติกรรมการเปิดเผยตัวตนอันเป็นที่นิยมอย่างกว้างขวางในการสื่อสารออนไลน์ปัจจุบัน กรณีที่สอง การเผยแพร่ข้อมูลส่วนบุคคลของผู้อื่นโดยมิได้รับความยินยอม ซึ่งส่งผลกระทบต่อสิทธิส่วนบุคคลอันเป็นสิทธิขั้นพื้นฐานที่สำคัญของมนุษย์ ดังนั้น งานวิจัยนี้จึงมุ่งศึกษาการปรับใช้มาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลในบริบทของการสื่อสารข้อมูลออนไลน์ ผลการวิจัยจากการวิเคราะห์ข้อมูลเชิงคุณภาพและการวิเคราะห์เนื้อหาเชิงเปรียบเทียบระหว่างกฎหมายไทยและกฎหมายต่างประเทศ ชี้ให้เห็นว่า ในปัจจุบัน ไทยยังไม่มีกฎหมายเฉพาะเกี่ยวกับการคุ้มครองสิทธิส่วนบุคคลและข้อมูลส่วนบุคคล แม้ว่าจะมีกฎหมายหลายฉบับที่อาจนำมาปรับใช้ในการคุ้มครองสิทธิส่วนบุคคลจากกรณีเผยแพร่ข้อมูลส่วนบุคคลในการสื่อสารข้อมูลออนไลน์ งานวิจัยนี้พบว่า ยังมีปัญหาในเชิงเนื้อหา องค์ประกอบ และขอบเขตหลายประการอันทำให้กฎหมายดังกล่าวยังไม่เหมาะสมและเพียงพอในการนำมาปรับใช้เพื่อคุ้มครองสิทธิของผู้ได้รับผลกระทบจากการเผยแพร่ข้อมูลส่วนบุคคลในการสื่อสารออนไลน์ งานวิจัยนี้จึงได้มีข้อเสนอแนะเพื่อปรับปรุงแก้ไขกฎหมายอันจะนำไปสู่การลดผลกระทบจากการเผยแพร่ข้อมูลและการคุ้มครองสิทธิส่วนบุคคลอย่างเหมาะสม

คำสำคัญ : สิทธิส่วนบุคคล การคุ้มครองข้อมูล การเผยแพร่ข้อมูลส่วนบุคคลออนไลน์

Introduction

The users of online communication such as internet, social network websites and Chat applications on mobile phone, deliberately or inadvertently share data in every aspects of life. The data shared includes image, telephone numbers, mailing addresses, workplaces, etc. which are considered “personal data” of an individual. The details of individuals’ activities have been published on a routine basis including private and intimate aspects of their lives. Not only personal information of the users of online communication has been published by themselves, but also that of non-users has been exposed online with or without their consent. Social network websites are one of the most popular data sharing platforms among Thai people. They allow an individual to construct personal profile which can be either public or semi-public profile within a system, whereby people can share and view profiles made by other users in the system. Social network websites vary in terms of goals, functionalities, and appearance of the different applications. The widely used social network websites in Thailand include Blogs, Facebook, and Twitter whereby the users share personal data relating to their daily life. Apart from text and images, the users can distribute video file and real-time communications. The details of the individual’s activities that have been published on a routine basis of daily life include private and intimate aspects of their lives. Apart from sharing their own personal data, social media users also share personal data of others.

This research has classified the sharing of personal data online into two main categories. First is the sharing of one’s own data which is associated with “self disclosure” behavior that becomes popular trend online. Second is the sharing of other’s personal data. On the one hand, the sharing of personal data online can enhance personal relationship and facilitate electronic commerce. On the other hand, the practice of sharing personal data online could lead to considerable risks and negative consequences especially the identity-related crimes. Besides the economic and financial damages that may result from the sharing of personal data, the abuse of personal data obtained online could cause damages to emotions and reputations. In addition, the sharing of others’ personal data online without consent

is against the right to privacy which is a fundamental right of humans. These negative consequences lead to the study of legal protection of privacy and personal data. In line with this idea, the research aims to study the application of the U.S. laws relating to the protection of personal data in the context of online communication. These foreign laws are examined in order to conduct a comparative analysis to Thai laws. This could lead to the proposal of suggestions for Thai government in amending related laws and enacting new specific laws for protecting the right to privacy in case of sharing personal data online.

With an aim to report on the application of Thai laws with respect to sharing personal data online, this paper will start by examining the literatures which consisted of three literature types. First, literature on the concept of the right to privacy as a basic legal framework for this research will be reviewed. Second, literatures relating to "self-disclosure" will be reviewed. Third, literature relating to the negative effects of personal data's sharing online will be studied.

The purpose of the research

1. To study the theoretical concept relating to the protection of the right to privacy in personal data sharing and associated risk.
2. To study the application of foreign laws, i.e., the U.S. and the E.U., relating to the protection of personal data shared online.
3. To study Thai laws relating to the protection of personal data shared online by comparing to the foreign laws with an aim to lead the comparative analysis to recommendations for adapting Thai laws to protect personal data shared online.

The scope of research

The scope of this research covers the content analysis of relevant laws including Thai Civil and commercial Code, Thai criminal code and specific Act i.e., the Computer-Related Offence Act B.E. 2550 and the "Official Information Act", B.E. 2540. The foreign laws to be analyzed include the relevant laws of the U.S. and the E.U.

Research Methodology

This research was conducted with the aim to study the application and interpretation of laws relating to the protection of personal data shared online. It employed the qualitative research approach in examining related documents including laws, court cases, and opinion of legal scholars. Such documents were analyzed by content analysis method. In addition, a comparative analysis was applied by comparing the content of Thai to the relevant U.S. and EU laws.

Literature Review

The literature review included three main groups. Firstly, literatures demonstrating the concept of the right to privacy provided a basic legal framework for the study. Secondly, literatures relating to the "self disclosure" behavior of users was examined as this becomes a significant trend in online communication. Thirdly, literature relating to the risk and negative effects of personal data shared online was reviewed.

The right of social network users to personal data protection is mainly based on concept of the right to privacy. This right has been referred to as "right to be let alone" i.e., right not to be interfered by others. (Warren and Brandies, 1890) Haag (1971) described the right to privacy as the right of exclusive access. This right excluded others from certain activities such as watching, intruding and utilizing personal data. Allen (1988) also argued that the limitation is the critical elements for the application of this right. This can be compared to the limited-access theory proposed by Godkin (Caudill, 1992) Additionally, Wacks (1989) indicated that an individual has his own territory where he can live without interference by others. Donnelly (1982) compared this right to human right that all human being were born with. Similarly, Alderman and Kennedy (1997) commented that the right to privacy related to personal rights that focused on the individual's dignity. However, the right to privacy is not an absolute right. Birkinshaw (2001) distinguished between the private sphere and the public sphere and commented that the right to privacy was limited in the public sphere. There are several dimensions of privacy. For example, Gavison (1980) introduced three aspects of privacy, i.e., secrecy, anonymity and solitude. Hendricks, Hayden and Novic (1990) found that right to privacy can be

classified into several subcategories such as right to self-determination, right to communicate, right to family, right to life. Posner (1998) explained that there are two main aspects of privacy. The first one was the right to be let alone. The second one was the right to concealment of information which, basically, was the collection and dissemination of personal data without consent that could be regarded as an invasion of privacy (Kanathip, 2014) In addition, the right to privacy is a dynamic right which can be evolved over time. Thus, the changing trend of human communication by using social media leads to the new claim of the right to privacy (Kanathip, 2012) especially the privacy of personal data disseminated through social media. Thus, the sharing of personal data of others without content is basically considered to be an invasion of privacy.

Secondly, online communication users always share their own personal data on a routine basis. Basically, this is not against the right to privacy because it is their own data shared out of their intention. However, the data can include personal data of others e.g. a story of oneself can involves names and addresses of others. Thus, this part will examine the literatures related to self-disclosure. According to the literatures, causes of self-disclosure can be explained by several theories. In the "Social Exchange Theory", the relationship of person is based on the subjective evaluation of benefits and costs. (Homans, 1958) As for the benefits expected from self-disclosure, there are both financial and non-financial benefits. Regarding financial or economic benefits, business sectors offer benefits such as discount in order to persuade individual to disclose personal information on social network websites in exchange for such benefits. Furthermore, non-financial benefits play a vital role in encouraging individual to disclose personal information. These benefits mostly relate to personal relationship which include mutual empathy, trust building and reciprocation in the context of personal relationship. (Joinson and Paine, 2007) Boyd (2007) pointed out that "self-presentation" as evident in user profile in social network websites, is an important incentive for disclosing personal information. Rosen and Sherman (2006) argued that the important incentives are pleasure and enjoyment. The feeling of trust is also regarded as a cause encouraging self-disclosure. Social network users usually have trusted other users in their contact list

or “friend” even though they have not been physically met on the face-to-face basis. (Spiekermann, et al, 2010) In addition, the control perception can lead to the increase in self-disclosure. (Culnan and Armstrong, 1999) Some social network users believed that they can control their information by using technical tools such as privacy setting mechanism. Consequently, self disclosure behavior can be analyzed by a combination of several factors as discussed in this part.

Thirdly, the sharing of personal data online could lead to negative effect on user’s privacy especially the “identity related crime”. Solove (2003) pointed out that “the increasing use of personal information and the widespread transfer of information facilitate theft of identity at greater degree than traditional ways of privacy violation”. The Organization for Economic Cooperation and Development (OECD) defines identity theft as an illegal activity which involves the “acquiring, transferring, possessing, or using personal information of a natural or legal person in an unauthorized manner with the intent to commit, or in connection with, fraud or other crimes.” (OECD, 2008) In the US. there is a specific law regulating “Identity theft” i.e. the US Identity Theft and Assumption Deterrence Act (title 18, s. 1028 (a) (7) U.S.C.) This law imposes liability to anyone who “knowingly transfers or uses, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law”. In Europe, Mitchison et al. (2004) demonstrated that it occurs “when one person obtains data or documents belonging to another, or the victim, and then passes himself off as the victim”. In this research, the term “identity related crimes” is used to cover all activities that target on personal data in the context of online communication. The impact of such crime can be found on several aspects especially those of financial and economic nauture. (Conkey, 2007) In addition, this crime causes other kinds of losses such as time spent on resolving the problems and legal issues (Barker et al., 2008, Listerman and Romesberg, 2009) The crime have also affected customer perception by undermining trust in modern method of payment, e.g. credit cards, online-payment, electronic banking. (Benton et al., 2007, Jonker 2007) This perception could have a negative impact on the growth of the online

business industry as a whole (Sproule and Archer, 2010) Apart from the financial aspects, the identity related crimes have an impact on the right to privacy of individual who exchange information online. The right to privacy is basically violated when personal data were shared online without the consent of such persons. Although the sharing of one's own data based on "self-disclosure" behavior does not violate the right to privacy due to the consent given by data owner, such sharing could post a threat of identity related crimes to data owner. Consequently, the sharing of personal data online could potentially lead to an identity related crimes which could not only affect data owner but also cause a financial and economic impact on the country.

Results

1. In the context of online communication including internet, chat application on smartphone and social network websites, this research has classified the sharing of personal data online into two main categories. Firstly, the sharing of one's own data is associated with "self disclosure" behavior that becomes a popular trend online. Basically, the sharing of one's own personal data does not violate the right to privacy on the ground that the data owner voluntarily and deliberately reveal his personal data. However, the self disclosure could lead to several kinds of online crimes including those related to identity. Thus, there should also be legal measures for protecting the data owners as well. Secondly, the sharing of others' personal data without consent evidently violates the right to privacy of data owner. From a legal perspective, this research revealed that there were no current Thai specific law enacted for protecting personal data shared online. A comparative examination indicated that in some countries such as the U.S. and the EU, there existed specific laws for protecting personal data online. Although there are some Thai laws that can be applied to protect personal data - e.g. the constitution, the criminal code, the civil and commercial code and the computer related crime Act- the results indicated several problems relating to the scope and elements which make them inappropriate to be applied for protecting personal data shared via online communication. Such problems will be later discussed.

2. At the constitutional level, this research found that Constitution of the Kingdom of Thailand B.E. 2550 (2007) recognizes the right to privacy in the context of personal data especially in section 35. Nevertheless, the subordinate laws and regulations are required in order to protect such rights. Currently, subordinate laws for protecting personal data in the context of online communication have not yet been specifically enacted. Furthermore, after the military coup in May 2014, the 2007 Constitution was repealed after which an interim constitution was enacted in July 2014 without any provisions related to the protection of the right to privacy.

3. Regarding the criminal code, this research indicated that sharing personal data via online communication could be deemed a criminally offensive as defamation according to section 326. However, the limitations of this offence is that it covers only the dissemination of data "in a manner likely to impair the reputation of other person or to expose such person to be hated or scorned". Thus, the mere act of sharing personal data online without any comments that is potentially harmful to reputation falls out of the scope of this offence. For example, one social media user has posted image or personal contact detail of the other on Facebook. This causes no reputational harm and the defamation law cannot be applied to protect person whose data were disclosed. Thus, a large number of personal data can be found online without appropriate legal protection of privacy right. Moreover, Thai criminal code has not stipulated the offence of identity theft.

4. This research found that the civil and commercial code of Thailand provides legal basis for individuals to initiate a claim against the abuse of personal data shared via online communication. Specifically, a general provision of tort law in section 420 can be applied to protect the right of individuals in general. In addition, if such dissemination of personal data is done in a manner that is harmful to reputation, section 423 can specifically be applied. This can be compared to the U.S. where tort laws can be applied to protect personal data. However, the main difference between Thai and the U.S. tort laws is that Thai tort law does not specifically stipulate the right to privacy while the U.S. tort law recognizes the right to privacy as specific tort. In addition, the U.S. privacy tort classifies invasion of privacy into several subcategories, i.e. intrusion upon seclusion, appropriation of name or

likeness and publicity given to private life. Such principles can be applied to protect personal data in the context of online communication. Furthermore, unlike the U.S. Tort laws which incorporate the punitive damage and enable individual to claim for emotional damage, Thai tort law does not embrace such principles. The compensation in a tort case mostly involves the physical damage which is tangible. Regarding the dissemination of personal data as a consequence of conflict, this research found that it could cause damage which is intangible such as the effect on emotion and feeling without any proof of financial damage. This makes current Thai tort law inappropriate for protecting the right to privacy in case of sharing personal data via online communication.

5. Regarding specific laws regulating computer crimes, this research found that Thailand has enacted the Computer-Related Offence Act B.E.2550 which regulates various cyber crimes. The results indicated that some offences stipulated in this law, especially section 14, can be applied in case of personal data shared online. However, some limitations were found, for example, the elements of section 14 are limited to cover only "forged or false" computer data. Then, importation into computer system of the personal data that are not forged or false is not punishable under section 14, though such data can cause reputational harm to other persons or affect the right to privacy of such person.

6. The "Official Information Act", B.E. 2540 (1997) could be regarded as specific law relating to the protection of personal data in Thailand. The main purpose of this law is to entitle individual the right to access public information in control of state agency. Hence, provisions of this Act mainly involve with the disclosure of public information (section 7, 9 and 11). However, this law provides the exception to the access of information especially in case of "personal information". In addition, this Act indicates the principles of protecting personal information in section 23, such as the collection limitation principle, the data quality principle, the purpose specification principle, use the use limitation principle. However, the critical limitation of applying this law to protect personal data disseminated via online communication is that the scope of this law merely covers personal information in possession or control of a state agency. Thus, this Act excludes information in

possession of private sectors such as internet service provider, service provider of social media, etc.

7. Concerning the comparative analysis of US and Thai laws, the results indicate that the U.S. does not have single privacy law regulating the collection and use of personal identifiable data. The related laws are fragmented and address specific sectors such as the collection, the use and the disclosure of personal information in baking and financial sector. (Jonathan, 1999) Compared to Thai law, current Thai specific law relating to the protection of personal informationis “Official Information Act, B.E. 2540 (1997). Although there are principles relating to the protection of personal data which include personal data shared via online communication, this research found a critical limitation of this as because it merely covers personal data in possession or control of a state agency. Thus, this Act excludes information in possession of private sectors including social media users. Recently, the Thai Government adopted the draft of the Personal Data Protection Bill in order to protect information privacy in relation to private sectors. However, this draft bill has not yet been enacted.

Regarding the U.S. privacy tort, the dissemination of personal data can be regulated by “intrusion upon one’s seclusion” or “public disclosure of private facts”. (Prosser, 1960) Thus, online communicators who share personal data of others without consent can be held liable under privacy tort. Unlike the U.S., Thai tort law does not specifically stipulate the “privacy” tort, then, the general principle of section 420 could be applied in case of sharing personal data. However, it is difficult for the plaintiff to prove damage occurring from such sharing especially in case of data disclosure without affecting reputation. Moreover, the sharing of personal data online such as via social network websites can lead to computer crimes especially identity theft. Comparing specific law for computer crime, the result demonstrates that both Thailand and the U.S. enacted specific law on this matter. The U.S. has enacted specific law regulating cyber crime, i.e. “the Computer Fraud and Abuse Act or CFAA (codified as 18 U.S.C., section1030). This law covers a wide range of cyber crimes. Specifically, it was amended by the “Identity Theft Enforcement and Restitution Act” in 2008 to include the identity theft relating to computer data. In

contrast, the Computer-Related Offence Act B.E. 2550 of Thailand provides no specific offences of identity theft relating to computer data.

8. Contrary to the US where the laws relating to data protection are fragmented, this research found that there is a main piece of law on data protection in the EU that covers the collection and use of identifiable personal data. By conducting comparative analysis of Thai and EU laws, this paper found that the main EU regulation relating to the protection of personal data is “European Privacy Directive 95/46/EC” which was passed in 1995 and came into force in 1998. This directive is commented as the most comprehensive international instrument of data protection laws (Swire & Litan, 1998; Bennett & Raab, 2006) The basic objectives of this directive consist of supporting the free flow of information in EU and protecting privacy. Some commentators argued that the goal of achieving an internal European market was elevated to the same level of fundamental human rights and more so, "The concern about privacy is totally subordinate to the market prerogatives". (Gutwirth, 2002) As for the objective to protect privacy, the personal data protection is regarded in EU as human right which should be protected. (Pearce and Platten, 1999) Then, it is evident that the Directive explicitly refers to the right to privacy. (recitals 2, 9-11, 68, art. 1(1)) The Directive 95/46/EC covers the protection of “personal data” defined as “any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity” (Art. 2(a)). Thus, personal data shared via online communication such as images, names, addresses, workplaces could be regarded as “personal data” because they can represent information on a person. Consent is a core principle under the notion of "privacy as control" (Westin, 1967). Only the data subject can decide if, when, and to what extent to open his or her virtual private sphere to other entities. Privacy Directive 95/46/EC (Article 7) stipulate this core principle. However, the Directive also provides exceptions to the principle of consent such as the collection of personal data is necessary in order to protect the vital interests of the data subject (art. 26(1)(e)). Then, a person who uses online communication is basically

required to obtain "consent" of the data subject before collecting and sharing of personal data. However, some scholars argued that consent is a highly volatile concept and subject to manipulation (Froomkin, 2000). As opposed to the EU, Thailand provides no specific laws to protect personal data. The only related law is "Official Information Act, B.E. 2540 (1997) which can merely regulate the collection and processing of data in possession of state agencies. Basically, it cannot be applied in case of dissemination of personal data through social media as a consequence of conflict. By contrast, principles in EU Directive can be applied to the collection and dissemination of personal data by both government and private sector such as the service provider of social network website. Hence, there are no principles such as "consent" and "notice" in Thai related laws as stipulated in EU Directive. As a result, users of online communication are not required to obtain "consent" before collecting and sharing of personal data. Thus, the personal data is widely and increasingly shared without sufficient legal protection and limitation.

Discussion and Conclusion

The users of online communication deliberately or inadvertently share personal data in all aspects of life. The data shared includes images, telephone numbers, mailing addresses and workplaces, etc. The sharing of other's personal data without consent obviously affects the right to privacy of the data owner which is regarded as fundamental or human right. In addition, such sharing could lead to identity related crimes. Although the sharing of one's own data based on "self-disclosure" behavior does not violate the right to privacy given by the consent of data owner, such sharing could include third party's data who does not give consent. Also, data owner could have the risk of falling victims of identity related crimes. Consequently, legal measures are necessary to be established in order to protect the right of those data owners. Nevertheless, the qualitative analysis of related laws demonstrate that there is no current Thai specific law enacted for protecting personal data shared via online communication. The comparative study indicates that in some countries such as the U.S. and the EU, there are specific laws for protecting personal data online. Although there are some Thai laws that can be

applied to protect personal data, the results indicated several problems relating to the scope and elements which make them inappropriate to be applied for protecting personal data disseminated on social media.

Based on these findings, the researcher proposes a main recommendation to Thai policy makers to enact and amend the laws. First of all, the enactment of specific laws to protect personal data is proposed. In this regards, the EU Directive could be considered as a model for drafting Thai data protection law. The main principles such as “consent” and “notice” should be incorporated. In addition, the researcher proposes the enactment of specific law regulating identity theft that stipulates the element of the offence and imposes criminal penalty to the criminal. This new law could take the elements of the US laws, i.e. the Identity Theft Deterrence Act and the Identity Theft Enforcement and Restitution Act as a model for drafting identity theft provisions in the specific Thai law. Apart from criminal penalties, the researcher suggests the amendment to Thai civil and commercial code by incorporating “privacy tort” as specific tort. This could assist Thai citizens in addressing civil cases to lodge claims for financial compensation entitled to emotional loss caused by personal data abuse. In this regard, the U.S. privacy tort could be taken into consideration for the elements of privacy tort. Besides the legal measures, the researcher also suggests Thai government agencies to educate and inform users of online communication of the importance of personal data and the risk associated with the sharing of such data online.

Reference

Alderma, Ellen & Kennedy, Caroline. (1997). *The right to privacy*. US: Vintage.

Barker, K. J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: awareness and prevention. *Journal of Financial Crime*, *15*(4), 398-410.

Benton, M., Blair, K., Crowe, M. & Schuh, S. (2007). *The Boston Fed study of consumer behavior and payment choice: a survey of Federal Reserve System employees.* Retrieved May 7, 2015, from http://www.bostonfed.org/economic/ppdp/2007/ppdp0701.htm

Birkinshaw, Patrick. (2001). *Freedom of Information : The law, the practice and the Ideal.* US: Butterworths.

Caudill, Edward. (1992, December). E. L. Godkin and his view of 19th century journalism. *Journalism & Mass Communication Quarterly*, 1039–1049.

Conkey, C. (2007). Assessing Identity-Theft Costs. *The Wall Street Journal - Eastern Edition*, (250), 3.

Culnan, M. J. & Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust. *An empirical investigation, Organization Science*, *10*(1), 104-115.

Donnelly, Jack. (1982, June). Human Rights and Human Dignity: An Analytic Critique of Non-Western Conceptions of Human Rights. *American Political Science Review*, (76), 303-316.

Gavison, Ruth. (1980, January). Privacy and the Limits of law. *The Yale Law Journal*, *89*(3), 421-471.

Gutwirth, S. (2002). *Privacy and the Information Age.* Oxford, UK: Rowman & Littlefield.

Haag, Van Den, Ernest. (1971). On Privacy. In J. Pennock & J. Chapman (Eds.), *Nomos XIII: Privacy.* (pp.149-168). New York: Atherton Press.

Hendricks E, Hayden T & J. D. Novik. (1990). *Your right to Privacy: A Basic Guide to Legal Rights in an information Societ.* US: Southern Illinois University Press.

Homans, G. C. (1958, May). Social Behavior as Exchange. *American Journal of Sociology, 63*, 597-606.

Joinson, A. N. & Paine, C. B. (2007). *Self-Disclosure, Privacy and the Internet, Oxford handbook of internet psychology.* Oxford, UK: OUP.

Jonker, N. (2007). Payment instruments as perceived by consumers - Results from a household survey. *De Economist, 155*(3), Retrieved May 14, 2015, from http://www.dnb.nl/binaries/Working%20Paper%2053_tcm46-146710.pdf

Kanathip Thongraweewong. (2012, May). Legal Measures for protecting the right to privacy: A study of invasion of privacy through the use of social network websites. *APHEIT Journal*, *18*(1), 39-51.

Kanathip, Thongraweewong. (2014). *State Telecommunication Surveillance : A Comparative Study of the US and Thai Telecommunication Privacy Laws, Conference Proceedings of the Forth International Conference on Digital Information and Communication Technology and its applications.* Retrieved June 16, 2015, *from* http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6821709

Listerman RA, Romesberg J. (2009). Are We Safe Yet?. *Strategic Finance, 91*(1), 27-33.

Organization for Economic Cooperation and Development. (2008). *OECD Policy Guidance on Online Identity theft*. Retrieved May 15, 2015, from http://www.oecd.org/dataoecd/49/39/40879136.pdf

Posner, Richard. (1998). *Economic analysis of law, (fifth edition).* U.S. : Aspen Law & Business.

Prosser, William. (1960, August). Privacy. *California Law Review*, *48*(3), 383-423.

Rosen, P. & Sherman, P. (2006). Hedonic Information Systems: Acceptance of Social Networking Websites, in Americas Conference on Information Systems, Mexico: Acapulco.

Solove, Daniel J. (2003, Fall/Winter). Identity Theft, Privacy, and the Architecture of Vulnerability. *Hastings Law Journal*, 1227-1275.

Spiekermann, Sarah, Krasnova, Hanna, Koroleva, Ksenia & Hildebrand, Thomas. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, *25*(2), 109-125.

Sproule S, Archer N. (2010, November). Measuring identity theft and identity fraud. *International Journal of Business Governance and Ethics, 5*, 51-63.

Swire, P. P., & Litan, R. E. (1998). *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive*. Washington D.C.: Brookings Institution Press.

Wacks, Raymond. (1989). *Personal Information : Privacy and the Law*. Oxford: Clarendon Press.

Warren, D Samuel & Brandeis, D. Louis. (1890). The Right to Privacy. *Harvard Law Review*, *IV*(15) Retrieved May 15, 2015, from http://www.lawrence.edu/fast/boardmaw.

Westin, Alan. (1967). *Privacy and Freedom*. New York: Atheneum.