PROTECTION OF MOBILE APPLICATION USERS' PERSONAL DATA*

*Warin Asavaratana***

ABSTRACT

At present, mobile apps become an important part of many people's lives. A study conducted in 2014 by twenty-six worldwide data protection authorities showed that there are three major data protection problems in the mobile app context. First, the mobile apps appear to request excessive access to personal data. Second, there is no notice about data protection policies that mobile app users could read before downloading such mobile apps. Third, mobile app users have no real control over their personal data.

Although Thailand has also been confronted by mobile app data protection problems, the existing laws are insufficient to govern such problems. Moreover, there have been attempts to pass personal data protection bills intended to deal with the data protection problems. However, if either of the bills were enacted, there would still be shortcomings causing mobile app data protection problems to remain unresolved.

This thesis aims to study on the problems of Thai law on mobile app data protection, analyze and compare to foreign legislations, namely Canada, the United States of America, and the European Union. In conclusion, this thesis proposes that a specific law providing mobile app developers' liabilities should be enacted and a specific authority handling data protection complaints should be established in order to govern the mobile app data protection problems.

Keywords: Data Protection, Mobile Applications, Data Protection and Privacy

บทคัดย่อ

ในปัจจุบันโปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่ (Mobile Apps) ได้กลายเป็นส่วนสำคัญในชีวิตผู้คนจำนวนมาก งานวิจัยในปี พ.ศ. ๒๕๕๗ ซึ่งจัดทำโดยหน่วยงานคุ้มครองข้อมูลจากทั่วโลกระบุว่าปัญหาหลักเกี่ยวกับการคุ้มครองข้อมูลในโปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่มีอยู่ ๓ ประการ ได้แก่ ๑. โปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่มีการขอเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้เกินความจำเป็น ๒. ไม่มีนโยบายเกี่ยวกับการคุ้มครองข้อมูลให้ผู้ใช้ได้อ่านก่อนที่จะดาวน์โหลดโปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่ และ ๓. ผู้ใช้โปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่ไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้อย่างแท้จริง

ถึงแม้ว่าประเทศไทยจะเผชิญปัญหาเกี่ยวกับการคุ้มครองข้อมูลในโปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่ก็ตาม แต่กฎหมายที่บังคับใช้อยู่ในประเทศไทยก็ไม่สามารถจัดการกับปัญหาเหล่านี้ได้ ทั้งนี้ มีร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจำนวน ๒ ฉบับอยู่ใน

* The article is summarized and rearranged from the thesis "Protection of Mobile Application Users' Personal Data" Master of Laws Program in Business Laws (English Program), Faculty of Law, Thammasat University, 2015.

** Graduate student of Master of Laws Program in Business Laws (English Program), Faculty of Law, Thammasat University.

ระหว่างการพิจารณา ซึ่งร่างพระราชบัญญัติเหล่านี้มีวัตถุประสงค์เพื่อจัดการกับปัญหาการคุ้มครองข้อมูล อย่างไรก็ตาม ไม่ว่าร่างพระราชบัญญัติฉบับใดจะได้รับความเห็นชอบออกเป็นกฎหมาย ข้อบกพร่องในร่างทั้งสองฉบับจะทำให้ปัญหาเกี่ยวกับการคุ้มครองข้อมูลในโปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่ไม่ได้รับการแก้ไขสืบต่อไป

วิทยานิพนธ์ฉบับนี้มุ่งศึกษาถึงปัญหาของกฎหมายไทยในการคุ้มครองข้อมูลในโปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่ วิเคราะห์และเปรียบเทียบกับกฎหมายต่างประเทศ ได้แก่ แคนาดา สหรัฐอเมริกา และ สหภาพยุโรป โดยสรุปแล้ว วิทยานิพนธ์ฉบับนี้เสนอให้มีกฎหมายโดยเฉพาะกำหนดความรับผิดของผู้พัฒนาโปรแกรมประยุกต์และให้มีหน่วยงานโดยเฉพาะกำกับดูแลข้อร้องเรียนเกี่ยวกับการคุ้มครองข้อมูล เพื่อที่จะจัดการกับปัญหาการคุ้มครองข้อมูลในโปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่

คำสำคัญ: การคุ้มครองข้อมูล, โปรแกรมประยุกต์สำหรับอุปกรณ์เคลื่อนที่, การคุ้มครองข้อมูลและความเป็นส่วนตัว

Introduction

At present, mobile apps become an important part of many people's lives. People who use this technology gain benefits from the great functionality of mobile apps. However, beneath the success of the mobile app business, there is a cost to users' personal data. A study[1] in May 2014, which was conducted by twenty-six worldwide data protection authorities by evaluating 1,211 mobile apps both iPhone and Android, concluded that, there are three major mobile app data protection problems. In brief, these three major problems are as follows:

1) The mobile apps appear to request excessive access to personal data based on users' understanding of mobile apps' functionality.
2) There is no notice about data protection policies and practices that users are able to read before downloading such mobile apps.
3) Users have no real control over their personal data.

The legal world relies on permission-based controls.[2] In case users download the mobile apps without the provided information about the type of personal data that will be collected, the purposes for which such personal data will be collected, and the identity of third-parties that the collected data will be disclosed to, such downloading could not be considered legitimate consent. Therefore, if users' personal data are accessed, stored, used, or disclosed without obtaining explicit and legitimate consent from such users, it shall be an infringement of the right to the protection of personal data. Moreover, the situation where users cannot control their personal data can lead to other problems such as identity theft, blackmail, junk mail, spam, unsolicited mails or messages.[3] At this point, mobile app developers are the key people for these data protection problems. They are the data

[1] Office of the Privacy Commissioner of Canada, "*Results of the 2014 Global Privacy Enforcement Network Sweep*", https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp. (last visited Oct. 9, 2014).
[2] Oliver Bray, *"The app effect: how apps are changing the legal landscape*", 19(2) **C.T.L.R.** 66 (2013).
[3] Clark D. Asay, "*Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*", 11 **Nw. J. Tech. & Intell. Prop.** 39 (2013).

controllers who determine the purposes and means of the processing of personal data.[4] Therefore, the mobile app developers are directly responsible and liable for any infringement of the right to the protection of mobile app users' personal data.

Canada and the EU already have specific laws providing mobile app developers' liabilities. They also have specific authorities enforcing and implementing their laws. In the USA, at a state level, especially in California, there are a supervisory authority and laws governing mobile app data protection problems. On the contrary, in Thailand, the existing laws are insufficient to deal with such problems. Moreover, there have been attempts to pass Personal Data Protection Bills. Even if either of the Bills were enacted, there would still be shortcomings causing mobile app data protection problems to remain unresolved.

Law Concerning Mobile Application Data Protection in Canada

In Canada, the Personal Information Protection and Electronic Documents Act ("PIPEDA") provides liabilities of mobile app developers and establishes the specific supervisory authority which handle data protection complaints arising from the mobile apps. In brief, the significant matters in the PIPEDA are as follows:

Mobile Application Developers' Liabilities

- Information

The mobile app developers have an obligation to provide the mobile app users with certain information about their data protection policies and practices before the mobile app users download such mobile apps. The specific information needed is as follows:[5]

(i) The identity of a person who is responsible for data protection practices, and a person to whom complaints about data protection issues will be sent.
(ii) The ways to access to mobile app users' PI collected by the mobile app developers.
(iii) A list of the type of PI that will be collected and a description of the purposes for which such PI will be used.
(iv) Information about the mobile app developers' policies; and
(v) A list of the type of mobile app users' PI that will be disclosed to third parties.

- Purpose Specification

The mobile app developers have to provide exact information about what are the purposes for which the PI is collected. Furthermore, the collected PI has to be only used for the identified purposes.[6]

- Data Minimization

The mobile app developers have to collect both the amount and the type of mobile app users' PI only that is necessary to achieve the specified purposes.[7]

---

[4] Article 29 Data Protection Working Party, "*Opinion 02/2013 on apps on smart devices*", 9, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[5] PIPEDA, sec 5, clause 4.8.
[6] PIPEDA, sec 5, clause 4.2.
[7] PIPEDA, sec 5, clause 4.4.

- Right of Access

The mobile app developers have an obligation to inform, upon request, the mobile app users of the existence, use, and disclosure of their PI. They also have to give the mobile app users access within a reasonable time period and at no expense if feasible.[8]

- Security

The mobile app developers have to apply security safeguards to protect the mobile app users' PI, which they have retained, against loss, theft, unauthorized access, use, disclose, duplication, or alteration.[9]

Supervisory Authority and Means of Handling Data Protection Complaints

By the virtue of the PIPEDA, the privacy commissioner of Canada ("the Commissioner") is the supervisory authority who is responsible for enforcing and implementing the PIPEDA. Their missions include handling data protection complaints.

In practice, when the mobile app users have found that their PI has not been handled in compliance with the PIPEDA, they can file a complaint with the Commissioner.[10] After that, the Commissioner may initiate an investigation of the complaint if the Commissioner is satisfied that there are reasonable grounds to investigate the matter.[11] Within one year, the Commissioner shall send the findings and recommendations to the mobile app users and the mobile app developers. Also, the Commissioner shall inform the mobile app users about the right to apply to the Court for a hearing concerning the complaint.[12] At this point, the Commissioner can get involved in a court hearing by obtaining consent from the mobile app users.[13]

Apart from any other remedies, the Court may order the mobile app developers to correct their data protection practices in order to comply with the PIPEDA, order the mobile app developers to publish a notice of any action taken to correct their data protection practices, or award damages to the mobile app users.[14]

Laws Concerning Mobile Application Data Protection in the United States of America

In the USA, there is no specific federal law concerning data protection in the mobile apps. However, at a state level, especially in California, there are laws concerning mobile app data protection. These laws are the Business and Professions Code of the State California Section 22575-22579 or the California Online Privacy Protection Act of 2003 ("Cal-OPPA") and the California Civil Code of the State California Section 1798.83 ("Shine the Light Law"). In brief, the significant matters in these laws are as follows:

Mobile Application Developers' Liabilities

- Information

[8] PIPEDA, sec 5, clause 4.9.
[9] PIPEDA, sec 5, clause 4.7.
[10] PIPEDA, sec.11 (1).
[11] PIPEDA, sec.11 (2).
[12] PIPEDA, sec.13.
[13] PIPEDA, sec.15.
[14] PIPEDA, sec.16.

The mobile app developers have to post their privacy policies.[15] Such privacy policies must meet the following requirements:[16]

(i) Identify the categories of PII the operators collect and the categories of third-party persons with whom the operators may share PII.
(ii) Explain how the consumer can review and request changes to PII if the process to review and request changes are available.
(iii) Describe the ways that the operators would notify consumers of changes to the privacy policy.
(iv) Identify the effective date of the privacy policy.
(v) Describe the ways that the operators provide "Do Not Track" options through web browsers.
(vi) Inform consumers whether other parties may collect PII across different websites over time.

- Right of Access

The mobile app developers have to provide, upon request, information about a list of the categories of PI disclosed to third parties and the names and addresses of the third parties that received such PI. Moreover, mobile app developers must also provide instructions about how mobile app users can make their disclosure request.[17] It should be noted that mobile app users can only request on the condition that the third parties shall use the disclosed PI for direct marketing purposes.[18]

However, the mobile app developers may be exempted from the aforementioned liability by adopting a privacy policy that allows mobile app users to opt-in or opt-out of the sharing of their PI.[19]

- Right to Object

The mobile app developers must provide the mobile app users the right to object disclosure of their PI to the third parties for direct marketing purposes. Moreover, the mobile app developers must also provide means to exercise this right free of charge.[20]

Supervisory Authority and Means of Handling Data Protection Complaints

With regard to the State of California, where the mobile app developers' liabilities are provided, the office of the Attorney General of California ("AG") is the supervisory authority who is responsible for enforcing the Cal-OPPA and the Shine the Light Law. Although the mobile app users can file a complaint about the mobile app data protection problems with the AG, the AG does not represent the mobile app users in personal legal actions. The mobile app

---

[15] Cal-OPPA, sec. 22575. (b).
[16] Kelsey Maxwell, "*Online Behavioral Advertising: The Pros and Cons of Regulation and Suggestions for Adherence to California's Constitutional Right to Privacy*", 19 **Nexus: Chap. J. L. & Pol'y** 60-61 (2013-2014)
[17] Privacy Rights Clearinghouse, "*California's "Shine the Light Law" goes into effect Jan. 1, 2005*", https://www.privacyrights.org/ar/SB27Release.htm (last visited April 17, 2015).
[18] *Id*.
[19] Shine the Light Law, sec. 1798.83. (c)(2).
[20] Tanya Forsheit, *"Is There a Pravicy Policy for that App?"*, 17, *available at* http://www.lacba.org/Files/Main%20Folder/Sections/International%20Law/InternationalLawNewsletter/files/privacyapp_forsheit_article.pdf.

users have to pursue remedies in their private dispute on the basis of tort law.[21] In conclusion, the AG shall file a lawsuit against a business which violates provisions provided in the Cal-OPPA and the Shine the Light Law. In addition, such a lawsuit does not aim to remedy the injured mobile app users.

Law Concerning Mobile Application Data Protection in the European Union

In the EU, the Data Protection Directive is a central piece of data protection legislation to which all EU member states must enact their data protection law pursuant. In brief, the significant matters in this Directive are as follows:

Mobile Application Developers' Liabilities

- Information

The mobile app developers must inform the mobile app users about certain information, such as the identity of the mobile app developers, the types of personal data that will be collected, the purposes for processing of the collected personal data, and the identity of the third parties in case such personal data are transferred.[22]

- Purpose Specification

The mobile app developers have to provide the purposes that are explicit and legitimate.[23] To be clear, the provided purposes must be specific regarding the processing of the mobile app users' personal data. Also such specific purposes have to be legitimate.

- Data Minimization

The mobile app developers must only collect the mobile app users' personal data that is necessary to achieve the specified purposes and not be excessive in relation to the specified purposes.[24]

- Right of Access

The mobile app developers must provide the mobile app users the right to access their personal data that are collected without unreasonable delay or expense.[25]

- Security

The mobile app developers are responsible to adopt appropriate measures in order to protect the mobile app users' personal data from alteration, destruction, loss, or unauthorized processing.[26]

Supervisory Authority and Means of Handling Data Protection Complaints

By the virtue of the Data Protection Directive, each member state of the EU has to provide that one or more supervisory authorities are responsible for monitoring the application of the Data Protection Directive.[27] The mobile app users can lodge a claim concerning any infringement of their rights under the national provisions adopted pursuant to

[21] State of California Department of Justice: Office of the Attorney General, "Protecting Consumers", http://oag.ca.gov/consumers (last visited Dec. 8, 2014).
[22] Data Protection Directive, art. 10.
[23] Data Protection Directive, art. 6 (b).
[24] Data Protection Directive, art. 6 (c).
[25] Data Protection Directive, art. 12.
[26] Data Protection Directive, art. 17.
[27] Data Protection Directive, art. 28, para. 1.

the Data Protection Directive. The supervisory authority shall investigate the claim in order to check on the lawfulness of data processing of the mobile app developers. When the investigation is complete, the mobile app users shall be informed of the outcome of the claim.[28] The supervisory authority is authorized to issue a warning to the mobile app developers, to order the blocking, erasure, or destruction of data, or to impose a ban on processing. Moreover, the supervisory authority can also engage in legal proceedings or bring the claim before the judicial authorities.[29]

Law Concerning Mobile Application Data Protection in Thailand and the Analyses of the Personal Data Protection Bills

The Existing Laws

- Civil and Commercial Code

According to Section 420, any person who violates other persons' rights is liable for the damage and is required to pay compensation.[30] Therefore, the mobile app developers must be liable for any infringement of mobile app users' personal data, such as disclosure of users' personal data without obtaining consent.

However, there are two shortcomings when apply this section to the mobile app context. First, the mobile app users have to prove that the mobile app developers violate their rights. At this point, it is burdensome for the mobile app users because it needs technical knowledge to show that there is an exploitation of their personal data. Second, even if they could prove this, it would be difficult to identify the certain damage or loss because most mobile app data protection problems cause emotional distress which is difficult to be converted to monetary form. Moreover, it appears that Thai Courts do not recognize this type of emotional damage.[31]

- Official Information Act B.E.2540

The Official Information Act B.E. 2540 provides almost the same data protection practices as the international standard.[32] However, this act only covers the personal information controlled or stored by state agencies or state enterprises. Thus, the mobile app developers are not subjected to this act.

- Computer Crime Act B.E.2550

Under the Computer Crime Act B.E. 2550, there are provisions providing mobile app developers' liabilities. Nevertheless, such provisions could be only applied to the mobile app context in certain circumstances and, therefore, cannot deal with the mobile app data protection problems sufficiently. The significant provisions are as follows:

---

[28] Data Protection Directive, art. 28, para. 4.
[29] Data Protection Directive, art. 28, para. 3.
[30] Civil and Commercial Code, sec. 420.
[31] จักรินทร์ โกเมศ, ค่าเสียหายสำหรับความเสียหายทางจิตใจตามกฎหมายลักษณะละเมิด, (วิทยานิพนธ์ปริญญามหาบัณฑิต, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2554) (Jukarin Komase, Damages for Mental Injury under Law of Torts, (LL.M. thesis, Thammasat University, Law, 2011)).
[32] Chungtong Opassiriwit, "*The Problem and Present Situation of Privacy Rights in the Digital in Thailand*", http://www.oic.go.th/content_eng/digital.htm (last visited Oct. 26, 2014).

Section 5[33] imposes penalties on illegal access to the computer system that has a specific access prevention measure. There are two shortcomings when applying this section to the mobile app data protection problems. First, the access has to be illegal, which means that such access is committed without obtaining consent.[34] Nevertheless, the mobile app users are the persons who give, by themselves, the consent allowing access to their smartphones. Second, this section is only applied to the smartphones that take specific access prevention measures. Thus, smartphones that have not taken such measures are outside the scope of this section.

Section 7[35] is similar to Section 5 but it imposes penalties on illegal access to the computer data instead of the computer system. It also has similar shortcomings. First, the mobile app developers usually dictate the data protection policies and practices by which they may access the mobile app users' personal data, thus their access to computer data is committed with consent. Second, this section is also only applied to the mobile app users' personal data that have taken specific access prevention measures.

Section 14 (1)[36] imposes penalties on inputting to a computer system fake computer data, either in whole or in part, or false computer data in the manner that is likely to cause damage to other persons or the public. With regard to the mobile app context, the mobile app developers might be subject to Section 14(1) in cases where they do not handle the collected personal data in compliance with the provided data protection policies because it could be considered they provides false statement in the policies. However, if the mobile app developers do not provide any policy at the beginning, they will not be subject to this section.

The Proposed Laws

In respect of the Personal Data Protection Bills, at the time of writing this article, there are two bills using the same title as "Personal Data Protection Bill B.E. …." The first bill has been introduced by the Official Information Commission (the Bill by OIC). Another bill has been introduced by the Electronic Transactions Development Agency (Public Organization) (the Bill by ETDA). Both bills are still in a stage of legislative process. Although the Bill by OIC and the Bill by ETDA are slightly different from each other in details, both bills provide mobile app developers' liabilities at nearly the same level as provided in Canada and the EU. The supervisory authorities, which handle data protection complaints, are also established by the virtue of both bills. However, both bills still have shortcomings causing the mobile app data protection problems to remain unresolved. In brief, these shortcomings are as follows:

1) Under the Bill by OIC, the definition of personal data is too narrow. The Bill by OIC places emphasis on information about the "identity" of persons. Therefore, the mobile app users' personal data, which are not related to the persons' identity, shall not be protected from unauthorized use and disclosure.

2) In both bills, there is no standard form of the notice about data protection policies in the mobile. Moreover, there are uncertainties about whether the mobile app developers can

---

[33] Computer Crime Act B.E.2550, sec. 5.

[34] ไพบูลย์ อมรภิญโญเกียรติ, **คำอธิบาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550**, น. 38 (พิมพ์ครั้งที่ 1 2553), (Paiboon Amornpinyokiat, **Explanation on The Computer Crime Act B.E.2550**, 38 (1st ed. 2011))

[35] Computer Crime Act B.E.2550, sec. 7.

[36] Computer Crime Act B.E.2550, sec. 14.

inform the notices in their website, or whether they have to make available links to notices on the page before downloading mobile apps.

3) The right to object to disclosure of personal data for direct marketing purposes is not recognized in both bills. The mobile app users have to face with a take-it-or-leave-it situation where they have to accept all the terms and conditions that are provided in the notices, otherwise they must not download such mobile apps.

4) The supervisory authority established by both bills does not help the mobile app users in pursuing remedies. The mobile app users have to pursue remedies on their own by filing a lawsuit with the Court. The problem in this point is that the mobile app users may not have enough technical knowledge to prove an infringement of their right to the protection of personal data and eventually their lawsuit might be dismissed by the Court.

5) If either the Bill by OIC or the Bill by ETDA were enacted into law, a number of mobile apps, which are developed in compliance with the Cal-OPPA, would be illegal. Because the mobile app developers' liabilities required by both bills are at a higher level than the mobile app developers' liabilities required by the Cal-OPPA. Consequently, Thai consumers shall lose opportunity to use such mobile apps.

Conclusion and Recommendations

A number of mobile apps have been found to access personal data at a greater level than is needed to operate their expected functions. Also, there are use and disclosure of personal data without consent from the mobile app users, and a failure to provide information about data protection policies and practices of such mobile apps. These problems can be considered an infringement of the mobile app users' data protection rights and have a significant impact on mobile app users' lives. Although there are laws concerning data protection in mobile apps in Thailand, the existing laws are insufficient to govern mobile app data protection problems. Furthermore, the Personal Data Protection Bills also have shortcomings which will cause such problems to remain unresolved.

After studying mobile app data protection laws in the foreign countries, namely Canada and the USA, and in the EU, and analyzing shortcomings in the existing Thai laws and the Personal Data Protection Bills, the writer would like to suggest the following points in order to be added to the Bill:

1) The meaning of "Personal Data" should be defined as identified or identifiable information about an individual.

2) The right to object to disclosure of personal data for direct marketing purposes should be recognized.

3) Certain information about the data protection practices should be presented in the app platform for the mobile app users to consider before they download such mobile apps. The form of this information must be well designed to fit smartphones' screens, not be lengthy, and inform, at a minimum, the following information:

- The type of personal data that will be collected.
- The use of such collected personal data
- Whether the collected data will be disclosed to third-parties or not
- If yes, the identity of third-parties.

Moreover, there must be a hyperlink to the whole content of the notice about data protection policies of such mobile apps in the app platforms as well. The notice shall explain the other information about data protection policies such as the identity and contact detail of the mobile app developers, the right of access or the right to object and how to exercise such rights.

4) The mobile app developers' liabilities should be applicable as the same level as provided in the Cal-OPPA. Moreover, such liabilities should be provided in a separate ministerial regulation.

5) The means of handling data protection complaints used in Canada should be adopted in the Bill. The Commission should be able to be involved in a lawsuit filed by the mobile app users by obtaining consent from such mobile app users.

REFERENCES

Books

ไพบูลย์ อมรภิญโญเกียรติ, **คำอธิบาย พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550**, พิมพ์ครั้งที่ 1. กรุงเทพมหานคร: โปรวิชั่น, 2553 (Paiboon Amornpinyokiat. **The Explanations on Computer Crime Act B.E.2550**. 1st ed. Bangkok: Provision, 2011.)

Articles

Asay, Clark D. "*Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*." **Northwestern Journal of Technology & Intellectual Property** 11 (2013): 321-356.

Bray, Oliver. "*The App Effect: How Apps Are Changing the Legal Landscape*." **Computer and Telecommunications Law Review** 19(2) (2013): 66-70.

Maxwell, Kelsey. "*Online Behavioral Advertising: The Pros and Cons of Regulation and Suggestions for Adherence to California's Constitutional Right to Privacy*." **Nexus: Chapman's Journal Law & Policy** 19 (2013-2014): 51-76.

Thesis

จักรินทร์ โกเมศ. "ค่าเสียหายสำหรับความเสียหายทางจิตใจตามกฎหมายลักษณะละเมิด." วิทยานิพนธ์ปริญญามหาบัณฑิต, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2554. (Jukarin Komase. Damages for Mental Injury under Law of Torts. Master's thesis, Thammasat University, Law, 2011.)

Electronic Media

Article 29 Data Protection Working Party. "*Opinion 02/2013 on apps on smart devices*.",<http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf> (accessed October 10, 2014).

Forsheit, Tanya. *"Is There a Pravicy Policy for that App?"*, <http://www.lacba.org/Files/Main%20Folder/Sections/International%20Law/InternationalLawNewsletter/files/privacyapp_forsheit_article.pdf> (accessed January 7, 2015).

Office of the Privacy Commissioner of Canada. "*Results of the 2014 Global Privacy Enforcement Network Sweep*.",<https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp> (accessed October 9, 2014).

Opassiriwit, Chungtong. "*The Problem and Present Situation of Privacy Rights in the Digital in Thailand*.", <http://www.oic.go.th/content_eng/digital.htm> (accessed October 26, 2014).

Privacy Rights Clearinghouse. "*California's "Shine the Light Law." goes into effect Jan. 1, 2005*.", <https://www.privacyrights.org/ar/SB27Release.htm> (accessed April 17, 2015).

State of California Department of Justice: Office of the Attorney General. "*Protecting Consumers*.", <http://oag.ca.gov/consumers> (accessed December 8, 2014).