ONLINE PROFILING AND DATA PROTECTION IN THAILAND[*]

Isaravadee Wongphasukchot[**]

Abstract

Online profiling has a major influence on global business opportunities. The use of online profiling primarily benefits digital advertising company as they can study users' behavior and other sensitive factors that could motivate the user to purchase, or show interest in products. It helps digital advertising company understands users' needs thoroughly and to distribute advertisements to target groups successfully. Online profiling might be used for encouraging, arousing or alerting users to buy, however, it could also be used to trick people by intruding on their personal privacy. This article examines the existing Thai law applied to the case of online profiling, significantly under the term which is not available in Thailand data protection bill, for example the definition of profiling, the concept of privacy impact assessment (DPIA), data breaches notification period and data protection officer. This article applies a comparative study and a comparison of existing approaches based on the General Data Protection Regulation (GDPR) and the American self-regulation Principles.

Keywords: Online Profiling, Personal Data Protection

[*] This article is summarized and rearranged from the thesis "Online Profiling and Data Protection in Thailand" Master of Laws Program in Business Laws (English Program), Faculty of Law, Thammasat University, 2017.

[**] Graduate student of Master of Laws Program in Business Laws (English Program), Faculty of Law, Thammasat University. Email address : isaravadee.w@gmail.com

1. Introduction

With the digital opportunities available to business marketing nowadays, there are a variety of online methods for marketers and entrepreneurs to use mass media to deliver and promote their products or services to customers. The way they communicate and attract people's attention is called "advertising". Although there is a wide range of advertising methods, the most effective method, and the one that has the least limitation, in order to reach potential consumers is digital advertising (internet advertising), Digital advertising evolves from delivering random products or services (random advertising) to a form of targeted advertising. The digital advertising that employs the method of behavioral targeting is called Online Behavioral Advertising (hereinafter "OBA"). OBA is a form of direct advertising typically associated with Internet users through various sources, for example profile information and social media or social networking websites. Online profiling is the primary step of OBA; refers to the digital advertising practice of collecting and predicting information with the main purpose of delivering advertising tailored to the user's interests, it is used before delivering the advertising to Internet users.

2. Overview of Online Profiling

Online profiling has been intensively used in advertising since the late 1990s. Many of the companies engaged in online profiling are so-called "advertising networks" or "network advertisers" (ad network). To demonstrate, on one side there is the website publisher looking to sell advertising impression space on a website, and on the other side is the advertiser who is looking for a channel to deliver ads. An ad network can also be called a broker (a neutral intermediary) between a group of publishers and a group of advertisers. The ad network applies technology to aggregate audiences, sells a packaged inventory to target customers (advertisers) and charges advertisers for serving their ads. Regarding the

relationship between the ad network and the publisher, the publisher allows the ad network to supervise the advertisements on the websites and decides on behalf of the publishers which ads should be placed there. Large ad networks typically work with thousands of different publishers[1], creating their own network, or list of partners, and occasionally the ad network and the publisher are the same entity. There are 5 stages explained the practice of online profiling: (1) installation of the technology; (2) tracking of the users; (3) collection of the data in private databases; (4) aggregation of the data; and (5) use of the profiles created after the aggregation of the data.[2]

3. Privacy Concern of Online Profiling

Based on their online behavior, a person will receive advertisements related to their activities or their preferences, for example a person may receive diet products or gym membership in the popup ads online, as a result of the ad network wanting to spur them to join an exercise class and improve their fitness levels, but this could also make them feel that they are unhealthy or need to lose weight,[3] which resulting in low self-esteem. On the contrary, profiling is unwanted if a personalized offer tempts a user to buy chocolate and they are trying to resist this because they have just started a diet. Another example is the discrimination issue, when a network advertiser offers a discount for a toy to one user but not to another user,

---

[1] Eric Siu, '53 Alternative Ad Networks to Open up New Channels of Growth in 2018' <https://www.singlegrain.com/blog-posts/pay-per-click/44-ad-networks-will-help-open-new-channels-growth/?cv=1> Accessed 15 July 2018

[2] Laura Garcia Vargas, 'Do They Want to Regulate Online Profiling?' (2017) Canadian Journal of Law and Technology (15 C.J.L.T.) P.2

[3] Information Commisioner's Office, 'Feedback Request – Profiling and Automated Decision-making' (V1.0, 06 April 2017) <https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf> Accessed 15 February 2018

because the first one had bought a similar toy the week before. The network ad might also use profiling to determine prices and terms for goods and services, which could lead to unfairly discriminate pricing by offering some certain people who have more ability to pay products or services at a higher cost that are less favorable than others.

The complexity of online profiling create a loopholes for demining the damages and remedies as it does not appear until it is in targeting on OBA, and even it does not use in targeting, does not mean the harm is not occur for example if the users does not receive the targeted ads or opt out from targeting advertising, it only prevents from seeing targeted ads, not prevent tracking itself. The reason behind data protection legislative and self-regulation is taking measures to prevent personal data. Data protection law shall create more practical matters to prevent people from being tracked and bombarded with unwanted marketing material from digital ads business.

4. Online Profiling in Foreign Countries

The practice of online profiling has been attentively discussed through various aspects in foreign counties. Data protection in the United States provides a friendly data protection to the marketing, rather than considering the rights of the data subject. The United States does not have a comprehensive law governing personal data in general; instead, it regulates sector-specific laws and highlights a combination of legislation, regulation and self-regulation, but in terms of Online profiling, they mostly encourage companies to create self-regulation. The FTC and several organizations attempted to create new practices in order to strengthen the data protection in online profiling, and the advertising industry continues to develop its self-regulatory program for online profiling and applies it to most companies doing business in the US such as Self-Regulation Principles for Online Behavioral Advertising, The NAI code of Conduct and etc.

Meanwhile, the concept of profiling has been recognized in the EU data protection law for a long period, both explicitly or inexplicitly defined until recently, The General data protection (hereinafter GDPR) become effective on 25 May 2018, and it was designed better protect data subjects, which had an impact on the digital advertising field and the concept of profiling is strongly prescribed and applied under this regulation. The major change of the GDPR affecting the "Online profiling" context is as follows. (1) GDPR introduce a new definition "Profiling" (2) GDPR increased territorial scope to any ad network provider whether inside the European Union or outside, which processes European data without considering the location or the nations of the company. (3) GDPR introduces mandatory data breach notifications, any breaches which are risky to the rights and freedom of individuals, the processor is responsible for sending the notification to the data controller and regulators within 72 hours from the time such breaches occur. (4) Data protection impact assessment (hereinafter "DPIA") shall be carry out regard to the processing which cause high risk for the fundamental rights of the data subject (5) Data protection officers (Hereinafter "DPO") is responsible for informing any activity of processing or profiling of personal data to the Data privacy agent (DPA).

5. Online Profiling in Thailand

Thailand's existing laws provide protection to personal data in quite specific circumstances, for example; Credit Information Business Act (B.E 2549) applied in case of banking and financial businesses, the Broadcasting and Telecommunications Services B.E. 2553 provides a protection against telecommunications, Computer Crime Act B.E. 2550 deals with the processing of personal data which is collected in computer systems.

The current problem in Thailand is the limitation of an existing applicable law that can be applied to a case of online profiling. Most of the law focuses on civil remedy, which compensates an injured person after the damage, by bringing the lawsuit to the court, such as breaches under article

420 of the Thai Civil and Commercial Code. Most of the data breaches cases are not protected under Thai CCC. Significantly, tort law provides tortious liability which solves the problems at the final stage.

The matter of online profiling is in the stage of a preventive measure whereby tort law and contracts under the Thai Civil and Commercial Code cannot reach. Thailand has no consolidated law to govern personal data protection in general. After the attempts to pass data protection law for almost 3 years, the enforcement of the Bill will enable Thailand to have data privacy in compliance with higher standard of data protection. However the concept of online profiling remains largely unregulated. The bill may need some changes, especially in the definition cover to online profiling, the requirement of data protection officer and the recitals term describing statements of fact that help to clarify and explain the reason for each section. With Regard to the fact that online profiling carries out particular processing of data operations; it is a useful way in implementing the bill to comply with the GDPR, and enacting it into a binding law. Due to the GDPR is a comprehensive law that emphasizes the proper context, specified and characterized in a general term, it could be said that comprehensive privacy laws can facilitate the Internet of things by establishing a uniform set of rules and potential regulations. As a result, the data protection is potentially developed under the GDPR. The most important fact is the EU law's enforcement definitely has consequences for Thailand related to the business field. The GDPR increased territorial scope to any ad network provider whether inside the European Union or outside, which processes European data without considering the location or the nations of the company. Therefore Thailand's companies will have to follow the GDPR inevitably.

6. Conclusion and Recommendation

The revised 2018 data protection bill has introduced certain concepts similar to those in the GDPR and quite well aligned to the GDPR

that play in shaping data protection. However, in the online profiling context, the bill does not regulate the definition of profiling and criteria related to online profiling are missing; the privacy impact assessment (DPIA) and the data protection officer (DPO). From the study, self-regulation has not yet been proven sufficient to fully protect the interests of users with regard to behavioral advertising according to lacking effective enforcement. However, the collaboration between the legislative law and self-regulation may be considered as a better solution. However, as a result, this will cause other ineffective consequences, such as an overlapping authority between the organization that supervise self-regulation and other main legal enforcers who enforce the data protection law. In the United States, the industry has been almost untouched by oversight. From the study, we have recognized that the core of Thailand's personal data protection bill aims to update the framework with international standards and to be consistent with the GDPR. The bill adopted many articles of the GDPR it shall be deemed that the situation of data protection law in Thailand is expected to comply with the GDPR.

A legislative approach to online profiling is not discreet at this time; taking the GDPR as a model provides a huge benefit for internet users. Even though Thailand is not a European Union member state, Thai digital ads companies may serve customers in the EU. Thailand must have a protection rule equivalent to, or greater than, the GDPR. If Thailand does not establish a higher standard of data protection, this could mean the losing of business opportunities for Thailand with any EU companies. In order to close the privacy gaps in Thai regulatory frameworks, there is a need of creating a supplementary legal framework to support online profiling operations; the following terms shall be a new requirement and provided in the Bill,

6.1 Data Protection Impact Assessment (DPIA): Online profiling takes place with regard to risks arising from the operation and have an effective impact on the data subject. A DPIA provides an efficiency preventive measure before online profiling takes place. A DPIA should be

prescribed in the bill consistent with the GDPR. Online profiling takes place with regard to risks arising from the operation and have an effective impact on the data subject. A DPIA provides an efficiency preventive measure before online profiling takes place. A DPIA could be required the controller to seek advice from the Thai data protection commission and they should monitor the performance of the DPIA.

6.2 Data Breaches Notification period: If personal data is obtained indirectly, the users shall be informed in suitable time or on the first communication with them, "without undue delay where feasible, not later than 72 hours after having become aware of a breach(under GDPR). It requires a notice when an organization collects personal information from individuals in online contexts.

6.3 Data Protection Officer: This roll of the DPO is important, especially for companies that process a large amount of personal data. The concept of a DPO does not appear under the Thai Bill, but it is necessary to add a separate section for the requirement and responsibility of DPOs.

DPOs shall be appointed by the online ad company who uses the technique of profiling or automated processing of personal data without regards to the company size matter. Therefore, digital advertising companies are struggling to position a data protection officer. However, for a company that does not use technology that would pose a high risk to the rights of a natural person does not need a DPO, such as a local bakery that processes data like e-mail addresses.

References

Journal

Laura Garcia Vargas Do They Want to Regulate Online Profiling? Canadian Journal of law and technology [15 C.J.L.T.]

Websites

Eric Siu, '53 Alternative Ad Networks to Open Up New Channels of Growth in 2018' <https://www.singlegrain.com/blog-posts/pay- per-click/44-ad-net works-will-help-open-new-channels- growth/?cv=1> Accessed 15 July 2018

Information Commisioner's Office, 'Feedback Request – Profiling and Automated Decision-making' (V1.0, 06 April 2017) <https://ico.org.uk/media/ 2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf> Accessed 15 February 2018