UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 2 Article 2

2014

# Eyes on the Road Program in Taiwan—Information Privacy Issues under the Taiwan Personal Data Protection Act, 31 J. Marshall J. Info. Tech. & Privacy L. 145 (2015)

Chen-Hung Chang

# EYES ON THE ROAD PROGRAM IN TAIWAN—INFORMATION PRIVACY ISSUES UNDER THE TAIWAN PERSONAL DATA PROTECTION ACT

CHEN-HUNG CHANG*

ABSTRACT

In Taiwan a nationwide highway electronic toll collection (ETC) system, launched in 2014, which uses radio-frequency identification (RFID) technology to conduct toll collection, and an unintended effect is that the ETC system functions as a massive vehicle surveillance program that captures drivers' location data. This article will discuss a number of incidents of data mismanagement by the ETC operator; these incidents underscore the salient information privacy concerns of individuals when an organization that handles so much personal data does not take privacy seriously and is ill prepared to protect the massive amount of data it possesses.

Moreover, the ETC case illustrates the conflicts of interest between data subjects and the government when the latter intends to use the location data of individuals for either criminal investigations or espionage activities. By analyzing the ETC privacy issues in three dimensions—ETC operator vs. drivers, ETC operator vs. government, and government vs. drivers—this essay will examine whether Taiwan's privacy laws are sufficient to adequately address the conflicts of interest among data subject, data controller, and the government. The ETC scenario further involves new privacy challenges presented by new technologies. Particularly important is the issue of geographical location (geo-location) data protection. This essay will examine the respective privacy rules under which corporations and the government may lawfully access drivers' geo-location data and evaluate whether such rules are adequate.

In the United States, geo-location data is also raising troubling privacy concerns. As a comparative perspective, it is worth exploring

the privacy issues concerning geo-location data under the Fourth Amendment. This article highlights the privacy doctrines previously outlined by the U.S. Supreme Court and examines whether they are still adequate to respond to privacy threats posed by new technologies. This article also provides a perspective for U.S. information privacy reform to better protect information privacy.

## I. INTRODUCTION

In January 2014, Taiwan officially launched a nationwide highway electronic toll collection (ETC) system, which is a distance-based toll collection system designed to allow highway users to drive through the toll plaza without having to slow down to pay the toll. The ETC system was built and is operated by a Taiwanese based company, Far Eastern Electronic Toll Collection Co, Ltd. (FE-Toll),[1] which was founded to undertake the construction and operation of the ETC system. FE-Toll won the bidding and was chosen by Taiwan's National Freeway Bureau (NFB) to build and operate the nation's first national highway ETC project.[2] By using radio-frequency identification (RFID) technology,[3] vehicles are required to install an electronic tag (eTag) to connect with the ETC system. When vehicles pass through the electronic collection gates, the driving distance and charges are automatically recorded. Moreover, the ETC system uses cameras equipped with an automatic license plate reader to scans and capture the license plate numbers of vehicles without an eTag to send a bill to the registered car owners to

---

* S.J.D. Candidate, American University Washington College of Law. Email: chihshein@gmail.com. I would like to thank Michael Carroll, Amy Tenney, and Leesa Klepper at American University Washington College of Law for their valuable comments and guidance on my research and writing of this paper. I would also like to extend my gratitude to Adam Florek, R. Joseph Cook and the production staff of Journal of Information Technology & Privacy Law for their assistance in preparing this paper for publication.

1. *Company Overview*, FAR EASTERN ELECTRONIC TOLL COLLECTION CO., http://www.fetc.net.tw/externalFETC/english/en_01.html (last visited July 28, 2014).

2. *Milestones*, FAR EASTERN ELECTRONIC TOLL COLLECTION CO., http://www.fetc.net.tw/en/milestones.html (last visited July 28, 2014).

3. Oleg Kobelev, *Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance through the use of Radio Frequency Identification Technology and the Need for Legislative Response*, 6 N.C.J.L. & TECH. 325, 326 (2004) ("RFID is a technology that allows companies and governments to implant tiny and virtually undetectable microchips or 'tags' with antennas into almost any product or animal, including humans. Predicted by MIT researchers to become the most pervasive computer technology in history, most RFID tags do not require any external power source and can transmit information via radio waves when the tag enters the reception field of the nearest scanner. RFID tags are commonly used to store an Electronic Product Code ('EPC') that assigns a unique identifier to every RFID chip, thereby allowing fast, efficient, and cost-effective inventory tracking.") (footnote omitted).

collect toll payment.[4] With the implementation of the ETC system, all traditional manpower tollbooths in Taiwan have been removed, and no manual fee collection lanes will be available.[5]

Although the original goal of the ETC was to shorten the travel time on highways by employing a stable and efficient electronic toll collection system across the country, unexpected privacy concerns have been expressed over the widespread collection of data by the ETC system. The issue concerns not just the information users are requested to submit to FE-Toll when signing up to join the ETC program, such as user name, address, national identification number, car registration, and credit/debit card numbers for toll charges. ETC is more than a check-out counter for the use of highway services. Numerous electronic gates have been installed on the highways to conduct electronic surveillance on all vehicles entering the highway 24 hours a day, 365 days a year. To perform the task of collecting e-tolls, the ETC device monitors and records vehicles' use of the highway, including the date, time, distance driven, location, and movement of the vehicle.[6] An unintended effect is that the ETC system functions as a massive vehicle surveillance program that captures drivers' location data. For the purpose of this article, driver data collected by FE-Toll, including personal identifiers and travel records, are collectively referred to as "E-Toll data."

The ETC system has posed threats to information privacy. This article will discuss a number of incidents of data mismanagement by FE-Toll, underscoreing the salient information privacy concerns of individuals when an organization that handles so much personal data does not take privacy seriously and is ill prepared to protect the massive amount of data it possesses. There are concerns over FE-Toll's mismanagement of data for purposes beyond toll collection without drivers' consent. Many companies, not only FE-Toll, are trying to maximize the benefit of personal data by treating personal data as a commodity for sale, sharing data with third parties, or using data to analyze and gauge customer behavior in a manner that deviates from the scope of data use originally agreed upon.

---

4. *See* 林浩昇 [Lin Hao Sheng], *每月上2次 不裝eTag行得通* [*Using highway without eTag is workable if you only access highway twice a month*], 蘋果日報 [APPLE DAILY] (June 10, 2013), http://www.appledaily.com.tw/appledaily/article/supplement/20130610/35073745/.

5. *See 國道計程上路 收費站「關門不關燈」* [*A Distance-based Toll Collection System Has Been Launched on Highway; Tollbooths Are Shut Down*], 自由時報 [LIBERTY TIMES] (Dec. 30, 2013), http://news.ltn.com.tw/news/focus/paper/742622.

6. *See* 朱致宜 [Zhu Zhi Yi], *個資看透透 徐旭東變「全民公敵」？* [*Personal Data Are Becoming Transparent; Shu-Shu-Dong Is the Enemy of All Citizens?*], 財訊 [WEALTH MAG.], Jan. 15, 2014, http://www.ettoday.net/news/20140115/316568.htm.

Tension over privacy is not limited to FE-Toll and drivers. It also arises between FE-Toll and public sectors when the latter attempt to access the vehicle surveillance database. On several occasions, the government has expressed interest in accessing the comprehensive location data to address national security concerns, to assist in criminal investigation, or to gathering political intelligence.[7] How companies should respond to these requests for access to personal data causes a dilemma between sustaining consumer trust in business and resisting pressure from the government. There are also issues regarding the limits of information sharing between private sectors and the government.

Moreover, the establishment of the ETC involves a combination of efforts from the private and public sectors. If we perceive this issue from the perspective that FE-Toll is entrusted by the government as a "contractor" to operate the ETC system, FE-Toll is a quasi-public utility when it is carrying out the highway fee collection task. This leads to the issue of government collection and use of personal data, and thus, privacy tensions arise between individuals and the government. The ETC case illustrates the conflicts of interest between data subjects and the government when the latter intends to use an individual's location data for criminal investigation or espionage activities. How to reconcile personal privacy with the interests of society is a complex issue, especially when an individual's interest can hardly have equal standing with the powerful public interest.

By analyzing the ETC privacy issue from three perspectives—FE-Toll vs. drivers, FE-Toll vs. government, and government vs. drivers—this article will examine whether Taiwan privacy laws, primarily the Taiwan Personal Data Protection Act (PDPA),[8] which is the national law governing information privacy protection, are sufficient to adequately address the conflicts of interest among data subjects, the data controller, and the government. This article identifies the problem under the PDPA that, although specific rules and legal obligations have been created for the collection, use and storage of personal data, a problematic exemption to these obligations will largely undermine the goal of data protection. A particular issue is that the PDPA allows

---

7. *See* 葉志堅 [Ye Zhi Jian], *ETC成監控系統？！ 警政署發文監控全民* [*ETC Turns to Be a Surveillance System?! The Criminal Investigation Bureau Sent Notice to Monitor All Citizen*], 今日新聞 [NOWNEWS] (Jan. 10, 2014), http://www.nownews.com/n/2014/01/10/1085265.

8. Personal Information Protection Act (2010) (Taiwan), *translated at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627 (The PDPA is originally in Taiwanese. The PDPA is also called Personal Information Protection Act in some Taiwan law databases when said law is translated in English. There is no official English version or translation of PDPA in Taiwan.)

companies and the government to be exempted from the data protection principles if a public interest is involved. Due to a lack of specific factors regarding when and how public interest may justify the breach of personal privacy, this exemption is prone to abuse for data controllers because, under the umbrella of public interest, it allows them to bypass the obligation to safeguard privacy and breach the promise of personal data protection. It is critical to draw a line for accessing personal data in the name of public interest to minimize the controversies through the misuse of technologies resulting in surveillance of citizens without probable cause.

The ETC scenario further involves new privacy challenges presented by new technologies. Particularly important is the issue of geographical location (geo-location) data protection. New technologies such as the ETC system have enabled the tracking of drivers' locations and movements and have generated a new category of personal information—geo-location data—that did not exist before mobile devices and Global Positioning Systems (GPS) became widely available. Compared to traditional personal identifiers, such as names, social security numbers or a person's physical characteristics, geo-location data seems to be non-personal because the data merely indicate the geographic data of the device (such as cars in the ETC case) and do not directly reveal the identity of a person. However, the fact that geo-location data can be easily linked to personal identifiers (in the ETC case, all ETC users are required to submit their personal identifiers along with the vehicle identifiers to FE-Toll) and can be used to single out an individual's location and movements has made it necessary to include geo-location data in the scope of personal data. The possibility of using geo-location to trace drivers' whereabouts makes the location-based data even more sensitive than traditional personal identifiers. All the complexity of privacy elements and the corresponding privacy rules of geo-location data were obviously not considered and anticipated when the PDPA was drafted. This article will examine the respective PDPA rules under which corporations and the government may lawfully access drivers' geo-location data and evaluate whether such rules are adequate.

## II. INFORMATION PRIVACY AND THE TAIWAN PERSONAL DATA PROTECTION ACT (PDPA)

### A. THE RIGHT TO INFORMATION PRIVACY UNDER THE TAIWAN CONSTITUTION

The Taiwan Constitution does not contain the word "privacy" but, the right to privacy has been upheld on numerous occasions by the

Taiwan Constitutional Court (Taiwan's highest court, which has the ultimate decision-making authority on questions of the Taiwan Constitution). The Taiwan Constitutional Court has recognized privacy as a constitutional right:

> The right to privacy, though not clearly enumerated under the Constitution, is an indispensable fundamental right protected under Article 22 of the Constitution because it is necessary to preserve human dignity, individuality, and the wholeness of personality development, as well as to safeguard the freedom of private living space from interference and the freedom of self-control of personal information.[9]

The Taiwan Constitutional Court further interprets the concept of privacy to expressly recognize the right to information privacy:

> As far as the right to information privacy is concerned, which regards the self-control of personal information, it is intended to guarantee that the people have the right to decide whether or not to disclose their personal information, and, if so, to what extent, at what time, in what manner and to what people such information will be disclosed. It is also designed to guarantee that the people have the right to know and control how their personal information will be used, as well as the right to correct any inaccurate entries contained in their information.[10]

In a recent dispute stemming from the conflicts of freedom of expression and the right to privacy, the Constitutional Court again recognized that the Taiwan Constitution protects the rights of individuals to have their personal information remain private.[11] This is not an absolute right, and the Court held that whether information privacy may override free press shall be subject to the examination of necessity and proportionality.[12]

---

9. J.Y. Interp. No. 585, at reasoning ¶ 17 (Dec. 15, 2004) (Taiwan), *translated in* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=585 (the quoted language is a translation from Taiwanese to English by the author).

10. J.Y. Interp. No. 603, at holding ¶ 1 (Sept. 28, 2005) (Taiwan), *translated in* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=603 (the quoted language is a translation from Taiwanese to English by the author).

11. *See* J.Y. Interp. No. 689, at reasoning ¶ 7 (July 29, 2011) (Taiwan), *translated in* http://jirs.judicial.gov.tw/eng/FINT/FINTQRY03.asp?Y1=2011&M1=&D1=&Y2=&M2=&D2=&cno=&kw=&btnSubmit=Search&sdate=20110000&edate=99991231&keyword=&page=3&total=35&seq=30.

12. *See* J.Y. Interp. No. 689, at reasoning ¶ 7 (July 29, 2011) (Taiwan), *translated in* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=689.

## B. TAIWAN PERSONAL DATA PROTECTION ACT (PDPA)

### 1. Background: From a Sector-Specific to a Comprehensive Model

Taiwan has the unique experience of having adopted two of the world's most common data protection regimes at different stages. The European Union (EU) took the lead in implementing comprehensive privacy data protection laws applicable to all types of personal data across all sectors.[13] On the other hand, the United States is a notable example of a government that protects personal data through a sector-specific framework with fragmental privacy laws covering certain information categories for specific industries.[14] In 1995, Taiwan enacted its first law specifically addressing requirements of the collection, processing, and use of personal data—the Computer-processed Personal Data Protection Act (CPDPA).[15] This Act incorporated the fair information privacy practices and principles developed by the Organization for Economic Co-operation and Development (OECD) in 1980.[16] CPDPA adopted a sector-based privacy model that aimed to regulate data processing by government agencies, hospitals, schools, and private companies in certain industries such as telecommunications, banking, securities, insurance, and credit investigation. These industries were required to register with the competent authorities before they could collect, process, and use automated personal data.[17] There are additional data privacy protection requirements to address the particular needs or problems in numerous laws, such as the Financial Holding Company Act,[18] the

---

13. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 908-12 (2009).

14. *Id.* at 913.

15. Computer-Processed Personal Data Protection Act, Presidential Decree Ref. No. ROC-President-(I)-Yi-5960 (1995) (Taiwan), *available at* http://law.moj.gov.tw/LawClass/LawOldVer_Vaild.aspx?PCODE=I0050021 (only the Taiwanese version of the Act is currently available).

16. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (the principles are the "Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle.").

17. Computer-Processed Personal Data Protection Act art. 3, cl. 7, Presidential Decree Ref. No. ROC-President-(I)-Yi-5960 (1995) (Taiwan), *translated in* http://twse-regulation.twse.com.tw/EN/law/DAT06.aspx?FLCODE=FL010627&FLDATE=19950811&LSER=001.

18. Financial Holding Company Act arts. 42-43 (2009) (Taiwan), *translated in* http://db.lawbank.com.tw/ENG/FLAW/FLAWDAT01.asp?lsid=FL006621.

Telecommunications Act,[19] the Tax Levy Act,[20] the Settlement of Labor Disputes Act,[21] the Protection of Children and Youths Welfare and Rights Act,[22] the Sexual Assault Crime Prevention Act,[23] and Mental Health Law.[24]

A recent trend is that technology advancement has enabled the widespread collecting, processing, and transmitting of personal data by any individual, company, organization, or group. This trend, along with the earlier fragmented approach of a limited data protection obligation to certain sectors of industries, falls short of the goal of data protection. Therefore, the Taiwanese government decided to establish an information privacy protection framework of strong overall protection laws, regardless of the industry of the data controllers, which is not limited to automatically processed data. The Taiwan Personal Data Protection Act (PDPA) was passed by the Legislative Yuan (the Congress) on May 26th, 2010, and has been in effect since October 1st, 2012.[25] The PDPA generally follows the privacy principles approved by the Asia-Pacific Economic Corporation (APEC) in 2004[26] and the 1995 EU Data Protection Directive.[27] The PDPA not only regulates private entities but also imposes rules for data collection, use, and disclosure by the public sector. This approach is supported by and is coherent with Taiwan's constitutional obligation to protect citizens' information privacy.[28] This empowers the government to take an active stance,

---

19. Telecommunications Act arts. 6-7 (2013) (Taiwan), *translated in* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL012763.

20. Tax Collection Act art. 33 (2014) (Taiwan), *translated in* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL005933.

21. Act for Settlement of Labor-Management Disputes art. 24 (2009) (Taiwan), *translated at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL014924.

22. The Protection of Children and Youths Welfare and Rights Act art. 21 (2011) (Taiwan), *translated in* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL024905.

23. Sexual Assault Crime Prevention Act arts. 9-10 (2011) (Taiwan), *translated in* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL004532.

24. Mental Health Act arts. 24-25 (2007) (Taiwan), *translated in* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL013543.

25. Personal Information Protection Act (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627.

26. APEC SECRETARIAT, APEC PRIVACY FRAMEWORK (2005), *available at* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

27. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter EU Data Protection Directive], *available at* http://www.dutchdpa.nl/downloads_wetten/dir1995-46_part1_en.pdf.

28. *See* J.Y. Interp. No. 689, at reasoning ¶ 6 (July 29, 2011) (Taiwan), *translated in http://jirs.judicial.gov.tw/eng/FINT/FINTQRY03.asp?Y1=2011&M1=&D1=&Y2=&M2=*

instead of leaving the matter to industry discretion, to lay out the foundations of privacy protection principles so that businesses will know which line they should never cross.

2. Content, Basic Principles and Problems of the PDPA

The PDPA comprises fifty-six articles and governs several key issues: notification requirement, data subject's rights, legitimate criteria for data collection, processing and use, international data transfer, data security, data breach notification, sanctions, and regulatory control (enforcement).[29] The PDPA offers an extensive protection scope to apply data protection obligations to all government agencies and private entities (defined as "a natural person, legal person or any other body").[30] Following this goal, that the PDPA should be able to encompass activities involving the processing of personal data as broadly as possible, personal data[31] in the PDPA is defined as a broad concept to encompass any sort of information that can be used to directly or indirectly identify, or makes possible the identification of a natural person.[32]

The PDPA recognizes that there may be circumstances where the application of the PDPA would be excessively burdensome on social activities. Exceptions are made where data are processed purely for personal or family activities, for video and audio data collected in public venues, or at public activities that are not linked to other personal information.[33] Among other requirements and obligations, the PDPA

---

*&D2=&cno=&kw=&btnSubmit=Search&sdate=20110000&edate=99991231&keyword=&page=3&total=35&seq=30.*

29. *See* Personal Information Protection Act (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627.

30. Personal Information Protection Act art. 2, ¶ 1, cl. 8 (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627 (the quoted language is a translation from Taiwanese to English by the author).

31. For purpose of this essay, personal data and personal information are used interchangeably and do not refer to different definitions.

32. The personal data protected under the PDPA include:

> [N]ame, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health checks, criminal records, contact information, financial conditions, social activities and/or other information which may directly or indirectly be used to identify a living natural person.

Personal Information Protection Act art. 2, ¶1, cl. 1 (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627 (the quoted language is a translation from Taiwanese to English by the author).

33. Article 51 of the PDPA excludes the following activities and data from the application of the PDPA: "1. When a natural person collects, processes or uses personal data purely for personal or family activities; and 2. The image or audio data that are

requires written consent from the data subject whose personal data is collected, processed, or used, with a few exceptions.[34] Before providing written consent, the data subject must be provided with adequate notice before the entity first collects personal data.[35] The data subject has the right to request that the data controller delete or stop using the personal data when the originally intended purpose no longer exists, unless the laws state otherwise or the data subject has given written consent.[36]

The PDPA was designed to provide an overarching protection of personal data with an extensive scope but has faced a number of problems regarding its implementation due to incorrect perception of the law. Some have expressed concern that the rules are not strict enough for certain data,[37]while others complain that the same level of strictness will discourage innovation in technology development.[38] The complexity is compounded because not all data is created equal. The value of data varies depending on the nature and the context of application, thus calling for different levels of privacy protection. Similarly, personal data is used for various reasons. For instance, the same health data may be applied for multiple purposes, ranging from generating commercial profits to supporting academic research. When non-sensitive personal data is at odds with public safety or the well-being of the country, it may be justifiable to breach an individual's privacy right in furtherance of the public interest. On the other hand, if

---

collected, processed or used in public venues or at public activities and are not combined with other pieces of personal data." *Id.* at art. 51, ¶1 (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627 (the quoted language is a translation from Taiwanese to English by the author).

34. *Id*. at art. 15-16, 19-20.

35. *Id*. at art. 8.

36. *Id*. at art. 11.

37. One example being health information which has the potential to disclose a vast amount of personal information. In the view that health data may lead to higher risk of privacy invasion than other types of data, more restriction on the use of health data are necessary. *See* Chen-Mei Fan Chiang, *Medical Research and Personal-data Protection—Take Japanese Epidemiology Research as the Basis*, 10 TECH. L. REV. 61, 104 (2013).

38. In Liu Zuo-Guo v. Taiwan Mobile, No. 103-Bei-Hsiao-1360 (Taipei Dist. Ct. Oct. 20, 2014), the defendant, Taiwan Mobile Co., Ltd. argued that the court wrongfully interpreted the Taiwan Personal Data Protection Act when it failed to note that the subject information in the particular case (which is the name of cell phone service provider that the plaintiff engaged services with) is less sensitive and shall not be subject to the same level of strictness of other personal data. The court's final decision that the phone service provider has invaded personal privacy has been challenged that it is likely to impede technological innovation. *See* 洪聖壹 [Hong Sheng-Yi], *M+Messenger遭判違反個資 台哥大：觀念錯誤、將上訴* [*M+Messenger Is Ruled by the Court to Have Violated the Personal Data Protection Act; Taiwan Mobile: the Judgment Is Incorrect And It Will File an Appeal*], 東森新聞雲[ETTODAY], Oct. 28, 2014, http://www.ettoday.net/news/20141028/418979.htm.

a country threatened by terrorism plans to establish a national biometric database, where all citizens will be required to submit their facial and other physical identifiers for national security or prevention of crime, it is much more difficult to justify a privacy breach. It will not be easy to strike a balance between these prominent interests.

This article notes that a fundamental concept should be clarified in which the comprehensive model is aimed to lay out bottom-line standards for privacy protection rather than replace all other advanced privacy legislations if more layers of protection are considered. As noted in the legislative rationale of the PDPA, the Act is to set out the general and minimum requirements of personal data protection. A correct understanding of Taiwan's information privacy law is that the PDPA shall function as the baseline privacy protection framework, with additional layers of regulations and rules applicable to particular industry sectors, types of data, or specific topics. With this concept in mind, in regard to balancing the conflicting interests between individual privacy and the free flow of personal data in complex scenarios, one should carefully take into account all the competing interests involved to seek a balance, instead of mechanically applying the rules. In the current PDPA, some of the rules are poorly written and fail to consider the various possibilities of conflicts between personal privacy and the ability to freely use personal information. One example is an exemption to obtaining consent from a data subject to collect or use of personal data for the public interest, which will likely undermine privacy protections, if one does not take notice of the different contexts of personal data involved and the public interest pursued.

## III. ETC'S INFORMATION PRIVACY ISSUES

A number of incidents of data mismanagement by FE-Toll have drawn concern over the troubling invasion of privacy of millions of drivers across the country. FE-Toll's mass surveillance of nationwide vehicle data comes at a time when the Taiwanese PDPA is newly implemented and provides a framework to examine whether the PDPA is sufficient to protect individuals' information privacy. This article notes that while many incidents occurred due to FE-Toll's lack of awareness of its data safeguard obligations and failure to train responsible employees for information handling practices, the ETC case underscores a number of loopholes in the PDPA, primarily an exemption to a "notice and consent" requirement[39] that could be

39. Most information privacy protection legal regimes in the world are developed under the control–driven notion, which focuses on the autonomy of the data subjects in deciding whether and how their data can be used. Information privacy protection policy is

misused by a government or private entity to act against or without drivers' consents in the name of public interest. A peculiar dimension for academic research in the ETC case is that the ETC system has the unintended effect of functioning as a massive vehicle surveillance program to capture drivers' location data. It raises issues that include whether the basic privacy principles should be the same when it comes to consent, notice, and data use requirements, in view that drivers in fact have no real choice but are mandated to accept the surveillance if they want to use the highways.

### A. CAN FE-TOLL USE DRIVERS' PERSONAL DATA FOR NON-TOLL-COLLECTION PURPOSES?

#### 1. The Violation of Use Limitation Principle

The highly anticipated ETC program did not have a good start, and one of the misconducts of FE-Toll's handling of personal data was the disclosure of drivers' personal contact information to others without the data subject's consent for unjustifiable reasons. Numerous drivers were incorrectly charged on ETC toll roads operated by FE-Toll.[40] Complaints range from double charges and incorrect rates to FE-Toll's mismanagement of eTag accounts by withdrawing prepaid amounts when the account owner had not yet traveled on the highway.[41] One of the outrageous mistakes that may lead to a violation of the PDPA arises from an incident where FE-Toll misread the plate numbers, failed to collect the toll fee from the responsible driver, and charged another driver instead.[42] When the driver received the wrong bill and contacted FE-Toll customer service for bill correction and a refund, FE-Toll instructed the complainant to contact the responsible driver directly for fee reimbursement.[43] In this incident, it would be much more sensible, for both customer service and data protection reasons, if FE-Toll

---

primarily built upon notice-and-choice (informed consent) and transparency of data collection and processing, to ensure data subject has full control over his own data. *See* Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 34 (2011); *see also* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013).

40. *See* 曾懿晴 [Ceng Yi Qing], *遠通重複扣款 還靈異飄移溢收 [FE-Toll Double Charges Toll Fees and Mischarges Fees from Non-ETC-User]*, 中時電子報 [CHINATIMES] (Jan. 7, 2014), http://www.chinatimes.com/realtimenews/20140107004296-260401.

41. *Id*.

42. *See* Shelley Shan, *Toll system passes review's second week*, TAIPEI TIMES (Feb. 21, 2014), http://www.taipeitimes.com/News/taiwan/archives/2014/02/21/2003584026.

43. *See* 藍悅真 [Lan Yue Zhen], *eTag繳錯錢 退費竟要自找車主 遠通恐違個資法* [*FEToll Fails to Abide By the PDPA—eTag User Wrongfully Charged by FE-Toll Has to Deal with the Real User for Fee Reimbursement*], 大紀元電子日報 [EPOCHTIMES] (Feb. 26, 2014), http://www.epochtimes.com/b5/14/2/25/n4092102.htm.

collected the fee from the responsible driver in any manner available instead of requesting that the customer settle the misconduct caused by FE-Toll. In this case, FE-Toll should be justified under the PDPA for using the drivers' (both the victim and the person charged) contact information and/or bank account information to adjust the fee charges because such data is meant to be used for matters relating to the use of the ETC system. Regrettably, FE-Toll chose to disclose one driver's personal information, including name, telephone number, and the fact of his travel on the freeway, and the amount payable, to another driver and asked them to settle the wrong fee charge themselves.

FE-Toll's unauthorized disclosure of personal data is not permissible under the PDPA and is subject to sanctions and government audits. Drivers submit their contact information, such as home and email address, telephone, and credit card information to FE-Toll when enrolling in the ETC program. The driver's name, telephone number and highway travel records are the "contact information" and "social activities which may be used to identify a natural person," which is defined as personal data under the PDPA,[44] and therefore, FE-Toll shall use such data only in line with the purposes for which the data were originally obtained, i.e., for FE-Toll to collect toll fees. The law is clear that personal data may be used only for the purposes for which it has been collected subject to the following exceptions where:

> 1. It is in accordance with law; 2. It is to promote the public interest; 3. It is to prevent harm to the data subject's life, body, freedom or property; 4. It is to prevent harm to other persons' vital rights and interests; 5. It is necessary for a government agency or a research institution to conduct statistical data analysis or academic research, provided that the data, after being processed by the data provider or disclosed by the data collector, can no longer be connected with a person's identity; and 6. Written consent has been given by the data subject.[45]

---

44. Article 2 of the PDPA defines Personal Information as:

> The terms used herein denote the following meanings: [T]he name, date of birth, I.D. Card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information which may be used to identify a natural person, both directly and indirectly.

Personal Information Protection Act art. 2, ¶ 1 (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627 (the quoted language is a translation from Taiwanese to English by the author).

45. *Id*. at art. 20, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

Asking the victim of FE-Toll's misconduct to settle incorrect charges that were FE-Toll's fault is far outside the toll-collection purpose. If FE-Toll failed to obtain consent from the driver for data disclosure, the only possible excuse for FE-Toll to use personal data outside the original scope is to claim that the processing is to prevent harm to the vital rights and interests of the driver who was charged the fees.[46] However, the "other persons' vital rights and interests" normally refers to circumstances of life or death and does not seem to be a solid ground to justify the data misuse in the above scenario. Without any other grounds to disclose ETC users' data, FE-Toll will be held accountable for its misuse of personal data and thus breaching the purpose of collection under the PDPA.

2. The Violation of the Security Safeguards Principle

Another ground of PDPA violation arises from FE-Toll's failure to train responsible persons for information handling practices. Clearly, the FE-Toll personnel, when handling the aforesaid wrongful fee charge complaint, had no understanding that they must maintain the confidentiality of ETC personal data. The PDPA requires data controllers to adopt proper security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed,[47] and the PDPA Enforcement Rules expressly prescribe that security measures include "providing training on data protection issues."[48]

3. The Enforcement of the Accountability Principle

The PDPA sets forth enforcement mechanisms for data breaches. First, the victim of data misuse has recourse *against* the wrongdoer for losses incurred.[49] The PDPA stipulates that the wrongdoers shall indemnify the aggrieved data subject for any loss as a result of data misuse unless the accused can prove that the breach was neither deliberate nor caused by negligence.[50] To lessen the burden of proof for the data subject, and in view that in a data breach it is normally not easy to quantify the damage, the law provides that if the actual amount of damage is not easy to quantify or to prove, the court may order a

46. *Id*. at art. 20, ¶ 4.

47. "Non-Government Agencies that handle personal data shall adopt proper security measures to prevent personal data from being stolen, altered, damaged, destroyed or disclosed." *Id.* at art. 27, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

48. *Id*. at art. 12, ¶ 2 (the quoted language is a translation from Taiwanese to English by the author).

49. *Id*. at art. 28-40.

50. *Id*. at art. 29, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

damage amount in the range of NT$500 to 20,000 (approximately $17 to $640 in U.S. dollars) for each violation for each claimant.[51]

A class action mechanism is available under the PDPA; twenty or more individuals who have suffered losses due to the same data breach incident may grant their litigation rights to a qualified association or foundation to initiate a class action. For class action claims stemming from the same incident, the total compensation amount is subject to a cap of NT$200 million (approximately $6 million U.S. dollars) unless a higher actual damage amount can be proven.[52]

In addition to civil liabilities, serious violations such as those relating to breaching data confidentiality or security to make personal gains and cause harm to data subjects' rights, constitutes a criminal offence that is subject to a maximum sentence of five years in prison and/or criminal fines of up to NT$1 million (approximately $33,000 U.S. dollars).[53]

Additionally, a data breach may trigger the competent authorities' investigation and enforcement actions. If a violation is confirmed by the competent authority, the data controller could face administrative fines of up to NT$500,000 (approximately $16,000 U.S. dollars) for each violation.[54] Moreover, depending on the seriousness of the data breach, the competent authority may order the wrongdoers to cease the illegal data-handling practices and delete all illegally processed data.[55]

In Taiwan, there is no single national data protection authority. A number of authorities have responsibility for overseeing and enforcing the PDPA. The Ministry of Justice is the primary sector responsible for the interpretation of the PDPA and writing regulations.[56] The enforcement powers of the PDPA are exercised by the respective sector regulators and city/county government. For FE-Toll's violation of the PDPA, disclosing driver's contact information and travel records to a third party, the PDPA has provided adequate enforcement mechanisms to hold FE-Toll accountable for its violation of information handling practices. At the time of writing, however, no enforcement actions have been brought against FE-Toll.

### B. IS ETC GEO-LOCATION DATA PROTECTED BY THE PDPA?

The ETC scenario further involves new privacy challenges

51. Personal Information Protection Act art. 28, ¶ 3, art. 29, ¶ 2.

52. *Id*. at art. 28, ¶ 4; art. 29, ¶ 2, art. 34 (the quoted language is a translation from Taiwanese to English by the author).

53. *Id*. at art. 41-42 (the quoted language is a translation from Taiwanese to English by the author).

54. *Id*. at art. 47.

55. *Id*. at art. 25.

56. *See e.g. id*. at art. 6, ¶ 2.

presented by new technologies, particularly regarding issues of geo-location data privacy.[57] The central aspect is whether geo-location data is protected under the PDPA. Under the operation of ETC, FE-Toll collects geo-location data including drivers' travel records, images, photos, their locations, and movements.[58] At first glance, geo-location data may be non-personal because the data merely indicates the geographic position of the vehicles that do not directly reveal the identity of a person. Moreover, the plate number, the date and time of passing the e-toll gates, and the driving distance of cars might seem to be information without any personal communication content. However, technological innovation has made it possible to perform complex data analysis and transform the traditionally non-content or non-personally identifiable information into identifiable data.[59] The fact that all ETC users are required to submit personal identifiers along with the vehicle identifiers to FE-Toll when enrolling in the system has made ETC geo-location data easily linkable to a specific driver. Even for those who do not voluntarily enroll in the ETC program (some choose not to purchase an e-Tag but still required to use the ETC system because all manual collection lanes have been removed), FE-Toll can still identify the drivers from the automatic license plate reader through the registered plate number.[60]

ETC geo-location data can be used to track drivers' locations and movements in real time and indicate a drivers' route, locations for

---

57. *See* PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 8 (2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf ("Today's technologies easily determine an individual's current or prior location. Useful location-based services include navigation, suggesting better commuter routes, finding nearby friends, avoiding natural hazards, and advertising the availability of nearby goods and services. Sighting an individual in a public place can hardly be a private fact. When big data allows such sightings, or other kinds of passive or active data collection, to be assembled into the continuous locational track of an individual's private life, however, many Americans [] perceive a potential affront to a widely accepted 'reasonable expectation of privacy.'").

58. *See* 朱致宜 [Zhu Zhi Yi], *個資看透透 徐旭東變「全民公敵」？* [*Personal Data Are Becoming Transparent; Shu-Shu-Dong Is the Enemy of All Citizens?*], 財訊 [WEALTH MAG.], Jan. 15, 2014, http://www.ettoday.net/news/20140115/316568.htm.

59. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information,* 86 N.Y.U. L. REV. 1814, 1841-45 (2011) ("Technology is now posing a considerable challenge to the [non- personally identifiable information] side of the dichotomy. Computer scientists are finding ever more inventive ways to combine various pieces of [non- personally identifiable information] to make them [personally identifiable information].").

60. *See* 林浩昇 [Lin Hao Sheng], *每月上2次 不裝eTag行得通* [*Using highway without eTag is workable if you only access highway twice a month*], 蘋果日報 [APPLE DAILY] (June 10, 2013), http://www.appledaily.com.tw/appledaily/article/supplement/20130610/35073745/.

shopping and travel, and other information related to personal livelihood; meaning such data may be more sensitive than traditional personal identifiers.[61] Therefore, it makes no sense to exclude the ETC geo-location data from the scope of the PDPA. Geo-location data is the result of modern technology and was obviously neither considered nor anticipated when the PDPA was drafted. Fortunately, the definition of personal data under the PDPA has the flexibility to encompass any information that can identify an individual regardless of the type of technology used. Under the PDPA, personal data is defined broadly as a concept to encompass any sort of information "which may directly or indirectly be used to identify… all activities involving processing of personal data person."[62] The fact that the ETC geo-location data can identify a specific person should qualify such data for PDPA protection.

One may argue that when people knowingly expose themselves to the public, any personal information generated from their public activities should not be subject to privacy protection. Indeed, the PDPA recognizes that there are circumstances where the application of the PDPA would lead to an excessive burden on social activities, and exceptions are made under Article 51: "1. When a natural person collects, processes or uses personal data purely for personal or family activities; or 2. The image or audio data that are collected, processed or used in public venues or at public activities and are not combined with other pieces of personal data."[63] The rationale of the exemption is that when individuals voluntarily disclose data about themselves, they have a lesser expectation of privacy, and therefore, it is not necessary to subject them to data protection laws as long as such data is not combined with other personal information to identify or that is identifiable to individuals.[64]

In the *ETC* case, it is true that the ETC monitors and cameras on the freeways, which are undoubtedly public venues, to capture the drivers' movements and locations.[65] However, we cannot ignore the fact that such driver and vehicle image data will be combined with the

---

61. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 702-16 (2011).

62. Personal Information Protection Act, art. 2, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

63. *Id*. at art. 51 (the quoted language is a translation from Taiwanese to English by the author).

64. *See* J.Y. Interp. No. 689, at reasoning ¶ 7 (July 29, 2011) (Taiwan), *translated in* http://jirs.judicial.gov.tw/eng/FINT/FINTQRY03.asp?Y1=2011&M1=&D1=&Y2=&M2=&D2=&cno=&kw=&btnSubmit=Search&sdate=20110000&edate=99991231&keyword=&page=3&total=35&seq=30.

65. *See* 林浩昇 [Lin Hao Sheng], *每月上2次 不裝eTag行得通* [*Using highway without eTag is workable if you only access highway twice a month*], 蘋果日報 [APPLE DAILY] (June 10, 2013), http://www.appledaily.com.tw/appledaily/article/supplement/20130610/35073745/.

drivers' personal information to identify the specific driver for toll-collection. The reason the ETC system monitors and records the locations and vehicle movement is to calculate the toll fee and charge such fees to the driver.[66] Therefore, it is difficult to argue that the ETC geo-location data will not be used in association with the driver's personal identifiers. Thus, a proper interpretation of the PDPA is that the ETC geo-location data shall not fall under the exceptions of Article 51, and the collection, processing, and use of such data shall follow the PDPA.

Another reason that the ETC geo-location data shall not be excluded from privacy protection is that drivers do not have a genuine choice in accepting ETC surveillance. There is no alternative highway that offers a non-electronic-toll service. Drivers do not voluntarily expose themselves to the ETC surveillance and do not have a real option of refusing surveillance without being deprived of the right to travel. Driving on roads is not equivalent to a complete forfeiture of privacy. One may realize that her movements can be seen by other people in public venues and that there are speed cameras deployed along the roads to detect and deter speeding and red light runners. Nonetheless, this expectation is far from being placed in a surveillance web. If there were a choice, some would certainly choose traditional tollbooths to avoid being monitored by FE-Toll because they value privacy more than the benefits of a shorter traveling time. We will have to consider the imbalance of negotiation powers between FE-Toll and drivers. If FE-Toll is not prepared to improve its information-handling practices and establish a comprehensive privacy program, then drivers' privacy cannot be ignored by the PDPA, whose aim is to offer basic data protection for all activities involving the processing of personal data as broadly as possible.

In the United States, collecting and using geo-location data is also causing troubling privacy concerns, and the U.S. Supreme Court's decision in *United States v. Jones* sheds light on this problem.[67] In 2012, the Court heard a privacy invasion claim stemming from the use of a *Global Positioning System* (GPS) tracking device to monitor the target driver's movements.[68] It was highly speculated that the Court would use this opportunity to clarify whether geo-location data is protected by the Fourth Amendment, and if so, what level of regulatory control and privacy protection shall be accorded to such data. However, the Court avoided this highly debated issue and resolved the claim with the common law property-based privacy doctrine that "[t]he

66. *Id*.
67. United States v. Jones, 132 S. Ct. 945 (2012).
68. *See generally Id.*

Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment" because placing a GPS tracking device on a car is equivalent to trespass.[69] Although the privacy question associated with geo-location data remains unanswered, the *Jones* decision provides a favorable ground for ETC drivers' privacy protection as far as geo-location data is concerned. Because the *Jones* Court has ruled that the police only invade privacy when installing a GPS device on the target's vehicle, there is no reason to allow FE-Toll to conduct unregulated surveillance of vehicles with the electronic collection gates and cameras because these devices are tantamount to a GPS device attached to each vehicle on the freeway. The privacy invasion by ETC is even more severe, because *Jones* relates to specific suspects and is limited to a certain period, while the ETC functions as an around-the-clock surveillance of all the nation's drivers. The proportionality element in ETC is weaker than in *Jones* because there is no crime-solving reason behind the electronic surveillance, and toll collection does not seem a justifiable reason to track a driver's every movement on the road, especially for those who do not choose to expose themselves to the ETC surveillance.

### C. CAN FE-TOLL SHARE ETC PERSONAL DATA WITH ITS AFFILIATED COMPANIES?

Naturally, corporations are trying to maximize the benefit of personal data by treating personal data as goods for sale, sharing data with third parties, or using data to analyze and gauge customer behavior. FE-Toll is no exception. FE-Toll belongs to one of the largest conglomerates in Taiwan, Far Eastern Group, whose business widely covers telecommunications, construction, financial services, sea/land transportation, petrochemicals and energy, hotels, and retail stores.[70] The group has also founded a number of private colleges, universities, educational institutes, and medical centers.[71] In addition to internal use for toll collection, FE-Toll has incentives to share drivers' personal data with its affiliated companies to pursue lucrative benefits to its entire group. Moreover, Far Eastern Group's far-reaching business is capable of integrating the overlapping consumer data to generate profiles of individuals. These profiles include medical and health data, real estate information, education records, financial data, shopping preferences,

69. *Id. at* 946.

70. FAR EASTERN GROUP (Taiwan), http://www.feg.com.tw/tw/business/index.aspx (last visited July 28, 2014).

71. *Id*.

and so on.[72] For instance, with the assistance of the advanced information technology and analysis tool developed by the telecommunication company in the Far Eastern Group, FE-Toll can monitor and analyze the E-Toll data to evaluate optimal areas for its affiliated hotel or department store companies to expand new locations. FE-Toll controls the most up-to-date traffic data and can easily furnish such data to its affiliated mobile service carrier for them to provide real time direction or mapping services to their customers, which other competitors cannot provide. FE-Toll can also supply the E-Toll data for its affiliated insurance company to decide insurance policy rates. For example, an insurance company may charge higher insurance rates for speeding drivers. FE-Toll can further utilize vehicle location information for its affiliates to deliver a wide array of services especially for targeted advertisement. Moreover, Far Eastern Group is actively expanding its business into China, which presents the primary national security threat to Taiwan. It gives rise to another concern that the E-Toll data of millions of Taiwanese citizens will be exposed to data security risk when the data is transferred outside of Taiwan's border. Inadequate exchanges and processing of data within the same group further makes drivers' personal data more vulnerable.[73]

As tempting as it may be for FE-Toll to utilize the E-Toll data for extra benefits besides its toll-collection business, all these desired secondary uses that are incompatible with the toll-collection purposes are prohibited under the PDPA without the affected individuals' written consent. The purpose-limitation principle under the PDPA expressly sets a boundary that personal data can only be used for the purposes the data was collected for and shall not be reused for other purposes.[74] However, there are six statutory conditions for legitimate data reuse: (1) in accordance with the law; (2) to promote public interest; (3) to prevent harm to the data subject; (4) to prevent harm to other persons; (5) for academic research where the data has been made anonymous; or (6) the affected individual has unambiguously given his written consent.[75] The PDPA does not offer relaxed rules of data sharing for data controllers and their affiliated companies. FE-Toll's desired sharing of data with its affiliated companies does not seem to fall under any of the first five criteria. For individuals' written consent, the consent has to be specific written consent made by the data subject after having been notified by the collector of the new purposes and

72. *Id*.

73. *Business Association Graph*, FAR EASTERN GROUP (Taiwan), http://www.feg.com.tw/tw/business/index.aspx (last visited July 28, 2014) (the quoted language is a translation from Taiwanese to English by the author).

74. Personal Information Protection Act, art. 20, ¶ 1.

75. *Id*.

scope of data use and the consequence of withholding consent.[76] The onus is on the controller to be able to demonstrate that proper consent has been obtained. Therefore, FE-Toll must obtain written evidence to demonstrate that it has disclosed the information-sharing practices and obtained consent from drivers that specifically permits FE-Toll to share the E-Toll data with its affiliates.

Requiring consent appears promising for privacy protection, but consent can be tricky to manage, and it is important to consider whether the consent is valid and freely given. This article has identified a particular problem in the imbalance of negotiation power between FE-Toll and drivers because, in the eyes of many drivers, they are in a subordinate relationship with FE-Toll. If the consent for data reuse and sharing is bundled with the right to use the highways, drivers do not have a genuine choice in withholding consent without suffering prejudices in using the highways. When ETC users click the 'I accept' button on the consent form, it is unlikely to be valid and freely given. Although the PDPA does not expressly state that the consent has to be freely given, a proper appreciation of data protection must encompass this element.

Moreover, if any of the affiliated companies with whom FE-Toll wishes to share data are located outside Taiwan, the cross-border flow of personal data are subject to limitations under the PDPA. The PDPA recognizes that the transfer of personal data to other countries requires special consideration and empowers the competent authority to restrict the international transfer under situations where:

> 1. It will prejudice any material national interest; 2. It is prohibited or restricted under an international treaty or agreement; 3. The country to which the personal data are to be transmitted does not have sound legal protection of personal data, thereby affecting the rights or interest of the data subjects; or 4. The purpose of transmitting personal data is to evade restrictions prescribed under the PDPA.[77]

Like FE-Toll, many Taiwanese companies transfer personal data cross-border to their regional hub that hosts data processing facilities. One of the common data export destinations is China. At the time of

---

76. The consent requirement, as it appears in the PDPA, is as follows:

> The written consent mentioned in Item 7 of Article 16 and Item 6 of Paragraph 1 of Article 20 means a specific written consent made by the data subject after having been notified by the collector of the new purposes and scope of data use and the consequence to withhold the consent.

*Id*. at art. 7, ¶ 2 (the quoted language is a translation from Taiwanese to English by the author).

77. *Id*. at art. 21 (the quoted language is a translation from Taiwanese to English by the author).

writing China is still developing its national data protection laws, and it is unclear whether China can offer an adequate level of privacy protection as the recipient of data transferred from overseas. If China cannot offer adequate privacy protection, the Taiwanese government may ban such international transfers.

### D. CAN FE-TOLL SUPPLY ETC PERSONAL DATA TO THE GOVERNMENT FOR PUBLIC INTEREST?

#### 1. How to Interpret the Public Interest Clause of the PDPA

The limitless opportunities afforded by online business and advanced technologies have inspired companies to utilize the gold mine of personal data as much as they can. In the meantime, such comprehensive records of citizens are becoming important resources for many government agencies to achieve their objectives, and there are an increasing number of occasions where government agencies are expressing interest in gaining access to the databases maintained by companies for reasons of national security, criminal investigation and prevention, or disease prevention or treatment.[78] How companies respond to requests from the government to access their own personal database is a dilemma between sustaining consumer trust in business and resisting pressure from the government. On the other hand, some businesses are offering to sell consumers' personal data for profit. FE-Toll is one of them. News reports revealed that on two occasions FE-Toll, before the inauguration of the ETC system had already made sales pitches to Taiwan's national criminal investigation agency, the Criminal Investigation Bureau (CIB), offering to sell the E-Toll data.[79] The CIB also once sought access to the ETC database for reasons of crime prevention.[80] The questions that arise are: Does the CIB have any legal grounds to obtain the E-Toll data from FE-Toll? Can FE-Toll refuse CIB access? Does the PDPA permit FE-Toll to sell E-Toll data? All these questions are associated with a problematic rule under the PDPA that allows companies and the government to be exempted from

78. *See* PRESIDENT'S COUNCIL, *supra* note 57, at 5-6 ("Current rules may allow government to purchase or otherwise obtain data from the private sector that, in some cases, it could not legally collect itself, or to outsource to the private sector analyses it could not itself legally perform. The possibility of government exercising, without proper safeguards, its own monopoly powers and also having unfettered access to the private information marketplace is unsettling.") (footnotes omitted).

79. *See* 林志青 [Lin Zhi Qing], *遠通2次報價憂個資法打住　刑事局持續協調 [PDPA Concerns Halted FE-Toll Two Offers to CIB, Negotiation Continues],* 蘋果日報 [APPLE DAILY] (Jan. 11, 2014), http://www.appledaily.com.tw/realtimenews/article/new/20140111/324266/.

80. *Id.*

some data protection principles if public interest is involved.[81]

Although FE-Toll is prohibited under the purpose limitation principle of the PDPA to sell FE-Toll data to the CIB outside the original data collection purpose,[82] it is arguable whether FE-Toll claims that the sale of data is for the public interest because such information is helpful for the CIB to investigate crimes and preserve public safety. This likely assertion is based on Article 20, Paragraph 1 of the PDPA, which states that personal data may be used only for the purposes for which it has been collected unless "1. it is in accordance with law; 2. it is to promote the public interest. . . ."[83] Currently, there is no clear interpretation or guidance as to what types of tasks meet the public interest condition.

There are a number of reasons the "public interest" condition under the PDPA should be interpreted strictly and only apply to very limited situations. The primary reason is that private sectors collect and use personal data to pursue their own business benefits and not the public interest. Therefore, public interest will be narrowly applied to exempt data collectors from their data protection obligations. For the public sector, it is their responsibility to perform tasks in the public interest and such activities are often in conflict with individual privacy. We therefore need a rule to decide under what circumstances public interests shall prevail over personal privacy. However, businesses generally have no official authority or power and are not burdened with public tasks. If private entities are not obtaining personal data for the public interest, it is illogical to allow the private sector to assert public interest as a legitimate ground to use personal data in violation of the data subject's will. In regard to choosing between business interests and the public interest, the former is naturally the first priority for private sectors. If the public interest clause is applied broadly at the collector's discretion, it is difficult to expect that businesses will protect the interests of the data subject when the businesses are lured by potential gain brought by reusing this data. It is no different to open a door for the private sector to use personal data without restrictions in

---

81. Personal Information Protection Act art. 20, ¶ 1 (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627.

82.

"The rights and interests of the data subject should be respected in collecting, processing or using personal information and the information should be handled in accordance with the principle of bona fide. It should not go beyond the purpose of collection and should be reasonable and fair."

Personal Information Protection Act art. 5 (the quoted language is a translation from Taiwanese to English by the author).

83. *Id*. at art. 20, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

allowing private sectors to process personal data for a purpose that is irrelevant and even opposite the originally specified purposes. Absent clarification of specific factors regarding when and how public interest may justify the breach of personal privacy, this exemption is prone to abuse by data controllers bypassing the obligation to safeguard privacy and breach the promise of personal data protection under the umbrella of public interest.

The theme of the PDPA is to seek a balance between the interest of the data controller in using personal data and the privacy of individuals in keeping the data private. The PDPA imposes the condition that collection, processing, and the use of personal data by the private sector is lawful when it is done with the permissible criteria listed in the PDPA.[84] For certain situations, lawmakers acknowledge that the likelihood of harming privacy is minimal, as in the case where data is obtained from public resources or the data is used as part of a contractual relationship, therefore allowing companies to collect, process, or use personal data with easy-to-meet conditions.[85] In other circumstances, where lawmakers recognize that, although there may be potentially negative impacts to privacy, there are greater interests in safeguarding the collection, processing, or use of personal data. In these outlined exemptions, the benefits of the collection and processing of personal data preempts privacy rights. The PDPA provides an exhaustive list containing six clauses that outline these situations:

> Personal data may be used only for the purposes for which it has been collected subject to the following exceptions where: 1. it is in accordance with law; 2. it is to promote the public interest; 3. it is to prevent harm to the data subject's life, body, freedom or property; 4. it is to prevent harm to other persons' vital rights and interests; 5. it is necessary for a government agency or a research institution to conduct statistical data analysis or academic research, provided that the data, after been processed by data provider or disclosed by data collector, can no longer connect with a person's identity; and 6. written consent has been given by the data subject.[86]

For the "public interest" clause, the PDPA is not intended to grant a broad authorization for companies to freely collect, process, or use personal data under the banner of public interest. If public interest is broadly interpreted, all other requirements in the exhaustive list that were designed to impose limits on data controllers' information gathering would become useless. A sensible approach to adequately apply these clauses is that if any of the other five clauses fit the specific

84. *Id.* at art. 19, ¶ 1.

85. *Id.*

86. *Id*. at art. 20, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

situations, they should apply in priority to public interest. Moreover, when public interest is the only applicable situation, the clause should take into consideration the particular interests of the affected data subjects and the benefits of using the subjects' data. When the value of subject data is greater, the public interest should be significant enough to justify the breaching of an individual's privacy rights.

2. Does FE-Toll Need to Inform Drivers When Supplying E-Toll data to the Government?

Assuming, in an extreme situation, that FE-Toll can disclose the data to other parties in the public interest, a sound protection to personal privacy is that the affected individuals shall be properly informed of such disclosure and have the opportunity to dispute the disclosure. Unfortunately, the PDPA does not expressly require the data controller to give the data subject further notice when data is reused under the statutory exceptions.[87] When the data controller uses the data outside the scope of the original purpose, the data subject may not even know his personal information has been shared with others. Under the current PDPA, the notification obligations are applicable only when data is first collected.[88] The PDPA stipulates that "a government agency or a non-government entity, when collecting personal data from the data subject pursuant to Article 15 or Article 19, must unambiguously notify the data subject the following information: '1. Name of the government agency or non-government entity, 2. The purpose of data processing . . . .'"[89] Article 9 goes on to say:

> A government agency or a non-government entity, when collecting personal data pursuant to Article 15 or Article 19 but the data are not obtained directly from the data subject, must notify the data subject of the source of their personal data and the information contained in Clause 1 to Clause 5 of Paragraph of the preceding Article, before it process or uses such data.[90]

It is important to note that the most important purposes of the PDPA is to ensure fair and transparent processing and to empower individuals to require full and accurate information of the collection and use of data. This article proposes that a consistent implementation of the fair and transparent principle is that, even for statutory exceptions for the use of data, for another reason without the data subject's consent and outside the scope of the original consent, the statutory

87. *Id*. at art. 20.
88. Personal Information Protection Act art. 8-9.
89. Personal Information Protection Act, art. 8, ¶ 1.
90. *Id*. at art. 9, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

reason shall be a new and separate data collection activity by the party who obtains such data. The original data holders shall still be held accountable for the notification requirements to communicate the new data collection activity to the affected individuals.

### E. CAN GOVERNMENT REQUEST FE-TOLL TO SUPPLY E-TOLL DATA?

#### 1. The Scenario of the ETC Privacy Issue

What would be the legal complications when the CIB requests that FE-Toll supply E-Toll data? Must FE-Toll comply with the CIB's request? The first source of law the CIB relies on is the Communication Security and Surveillance Act (CSSA), which authorizes the government's surveillance of electronic communications in the process of criminal investigation through electronic devices.[91] In Taiwan, the CSSA is commonly used by law enforcement to conduct electronic surveillance or obtain wiretaps in investigating suspects or criminal defendants.[92] The E-Toll data is collected and transmitted to and from the ETC electronic system and may be included within the scope of the CSSA, as said law defines communications as "1. symbols, texts, images, sound or other wired or wireless telecommunications that are sent, stored, transmitted or received via telecommunication equipment."[93] Article 5, Paragraph 1 of CSSA stipulates that:

> If there are sufficient facts indicating that the accused or suspects have committed the following listed criminal offenses that seriously [in]danger national security, economic stability or society orders, and there are sufficient reasons to believe that the communication records are relevant to the subject investigation and such records cannot or are difficult to be obtained from other resources, an electronic-surveillance approval letter will be issued.[94]

An electronic-surveillance approval letter shall be approved by the court before conducting any type of surveillance in order to protect individuals' interests.[95] The CIB claims to access the E-Toll data for the "prevention of crime," which means no crime has been or is about to be committed at the time the request is made. Because there are no

---

91. Comm. Sec. and Surveillance Act, art. 5, ¶ 1 (2014) (Taiwan), *translated in* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL012821.

92. *See* Chih-Jen Hsueh, *Criminal Penalties for GPS Tracking: A Case Study on Taiwan High Court Judgment No. 100-Shangyi-Tzi-2407*, 11 TECH. L. REV. 119, 133-36 (2014).

93. *Id*. at art. 3, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

94. *Id*. at art. 5, ¶ 1 (the quoted language is a translation from Taiwanese to English by the author).

95. *Id*. at art. 5, ¶ 2.

identified suspects or defendants at the time the CIB requested the E-Toll data, the legitimate criterion of Article 5 of the CSSA has not been met. Accordingly, if the CIB fails to substantiate that the data request is related to a specific criminal investigation activity, it does not have statutory grounds under the CSSA to access E-Toll data, and FE-Toll may refuse the CIB's data requests.

Strategically, the CIB has an alternative to obtain the E-Toll data by relying on another source of law by alleging that the E-Toll data constitutes non-content communications, which can be accessed without a court approved electronic-surveillance letter.[96] For personal information such as dialed phone numbers, email addresses, and similar information unrelated to the content, the Taiwanese government agencies often rely on a relatively lenient legal standard of the Telecommunications Act. The Telecommunications Act states that the provider of wire or electronic communications services or cable and internet services shall take all necessary steps to preserve records in secrecy unless the disclosure of such records is made in accordance with the applicable laws and regulations.[97] However, a separate regulation promulgated under said Act requires these telecommunication service operators provide government access to the records in their possession.[98] The regulation adopts a relatively easy-to-meet standard that only requires the applicant agency to state the necessity, reasonableness, and proportionality when requesting the records.[99] However, no detailed requirements are provided, and the regulation does not even require the applicant agency to provide specific and articulable facts about the intended purpose of the data access. The vagueness of the language of the regulation is often misused by government agencies to obtain individuals' private contact information from telecommunications firms.[100] The Telecommunications Act has

---

96. *See* 吳景欽 [Wu Jing Qin], *非關犯罪之通聯紀錄調取之疑義* [*Issues of Accessing to Personal Communication Records for Purposes Not Related to Criminal Investigation*], 今日新聞網 [NOWNEWS.COM] (Jan. 24, 2014), http://www.ettoday.net/news/20140121/318115.htm.

97. Telecomm. Act, art. 7, ¶ 1 (2013) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL012763.

98. *Id*. at art. 7, ¶ 1-2.

99. Reg. for Handling Requests from Competent Authorities for Comm. Rec., art. 3, ¶ 1 (2002) (Taiwan), *available at* http://law.moj.gov.tw/Law/LawSearchResult.aspx?p=A&k1=%E9%9B%BB%E4%BF%A1%E4%BA%8B%E6%A5%AD%E8%99%95%E7%90%86%E6%9C%89%E9%97%9C%E6%A9%9F%E9%97%9C%E6%9F%A5%E8%A9%A2%E9%9B%BB%E4%BF%A1%E9%80%9A%E4%BF%A1%E7%B4%80%E9%8C%84%E5%AF%A6%E6%96%BD%E8%BE%A6%E6%B3%95&t=E1F1A1&TPage=1.

100. *See* 吳景欽 [Wu Jing Qin], *非關犯罪之通聯紀錄調取之疑義* [*Issues of Accessing to Personal Communication Records for Non-Criminal-Investigation Purposes*], 今日新聞網 [NOWNEWS.COM] (Jan. 24, 2014), http://www.ettoday.net/news/20140121/318115.htm; *see*

been criticized for having loopholes that allow public sectors to conduct unreasonable surveillance.[101]

The insufficiency and past injustices of data protection under the Telecommunications Act can now be remedied under the PDPA since said Act took effect on October 1, 2012. The PDPA has provided minimum data protection requirements for all personal data, and therefore, if the CIB or other government agencies wish to gain access to the E-Toll data, they must comply with the PDPA. Under the PDPA, a public entity must have a legitimate purpose and have at least one of the following criteria to lawfully collect personal data: "1. It is necessary in the exercise of the official authority vested in the controller; 2. A written consent has been given by the data subject; or 3. The rights and interests of the data subject will not be jeopardized."[102]

The CIB alleged that it is exercising its official duty to obtain E-Toll data.[103] Indeed, engaging in criminal investigation is among the official powers of the CIB. However, whether there is a close and substantial connection between the bulk collection of E-Toll data and prevention of crime is doubtful. The requirement for necessity is an essential limiting factor to narrow government interference with private interests and is essential for judicial review.

A prior dispute regarding the Taiwanese government's desired plan to establish a national fingerprint database may shed light on the conflict between information privacy and the government's duty. The Taiwan Constitutional Court ruled a clause of the Household Registration Act requiring citizens to submit their fingerprints when applying for a national identification card is unconstitutional.[104] Similar to the CIB's contention of its intended bulk data collection for crime prevention, the rationale behind the fingerprints legislation is to

---

*also*林鈺雄 [Lin Yu Xiong], *濫調通聯紀錄何時了？* [*Time to Cease Abusive Access to Personal Communication Records*], 自由電子報 [LIBERTY TIMES] (Jan. 13, 2014), http://www.libertytimes.com.tw/2014/new/jan/13/today-republic2.htm.

101. *See* 吳景欽 [Wu Jing Qin], *非關犯罪之通聯紀錄調取之疑義* [*Issues of Accessing to Personal Communication Records for Purposes Not Related to Criminal Investigation*], 今日新聞網 [NOWNEWS.COM] (Jan. 24, 2014), http://www.ettoday.net/news/20140121/318115.htm.

102. Personal Information Protection Act, art. 15 (2010) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL010627 (the quoted language is a translation from Taiwanese to English by the author).

103. *See* 葉志堅 [Ye Zhi Jian], *ETC成監控系統？！ 警政署發文監控全民* [*ETC Turns to Be a Surveillance System?! The Criminal Investigation Bureau Sent Notice to Monitor All Citizen*], 今日新聞 [NOWNEWS] (Jan. 10, 2014), http://www.nownews.com/n/2014/01/10/1085265.

104. J.Y. Interp. No. 603, at holding ¶ 1 (Sept. 28, 2005) (Taiwan), *translated in* http://jirs.judicial.gov.tw/eng/FINT/FINTQRY03.asp?Y1=2004&M1=&D1=&Y2=&M2=&D2=&cno=&kw=&btnSubmit=Search&sdate=20040000&edate=99991231&keyword=&page=12&total=148&seq=116.

create a national fingerprint database that will undoubtedly benefit criminal detection and investigation. The goal may sound promising, but such a proposition suggests that all citizens are potential criminals, and therefore, it will be helpful to establish a nationwide fingerprint system to identify criminal offenders. Supporters of such legislature fail to note that there is an imbalance between the interest of the government in gathering fingerprints and interest of all citizens who are required to give up their information privacy for vague and open-ended objectives. It is also left unexplained whether fingerprint gathering is necessary and is the only method to achieve the desired end. For example, fingerprints found at the crime scene do not necessarily prove that the fingerprint owner is the person who committed the crime. For these reasons, the Taiwan Constitutional Court ruled that the household agency's bulk collection of all of Taiwan's citizens' fingerprints violates the principle of proportionality and is unconstitutional and must be ended.[105]

For the ETC situation, if the reason the government seeks the E-Toll data is to facilitate crime prevention, this reasoning is based on the same hypothesis that all vehicle users are potential criminals, and thus, obtaining E-Toll data can benefit crime prevention. However, without proper justification that the E-Toll data are necessary to fulfill the stated objectives, or that all other options have been exhausted and there is no other way to achieve the same purpose, the CIB's request to access the ETC database for general crime prevention (i.e., not for a particular investigation of criminal case) is not in line with the principle of proportionality. FE-Toll should reject such requests pursuant to Article 5 of the PDPA.[106]

Moreover, if a broad crime prevention purpose cannot justify the government's invasion of personal privacy, there is no reason to allow private sectors, such as FE-Toll, to sell E-Toll data to the CIB for the claimed crime prevention reason. This supports the above assertion that the public interest exception for private entities to use personal data for other reasons should be interpreted strictly and only apply to very limited situations.

### 2. A Comparative Law Perspective from United States Supreme Court Decisions

In the United States, geo-location data is also raising troubling privacy invasion concerns. In the 2012 case of the *United States v. Jones*, the Supreme Court faced privacy challenges presented by new devices when police placed a global positioning system (GPS) device on

105. *Id*.

106. Personal Information Protection Act art. 5.

a car to track the target's whereabouts for twenty-eight days.[107] Public activities and personal information a person puts into the hands of others are generally not protected under the U.S. Fourth Amendment.[108] However, new technologies such as GPS location identification function has blurred the line of "public" and "third party" elements because one may realize that his movements can be seen by other people in public venues, but his expectation is far from being put into a surveillance web and having every movement on the road recorded.[109] Surveillance in public and access to records held by third parties are new technology privacy concerns that call for new constitutional rules. Unfortunately, no good answer has been provided yet. As a comparative perspective, it is worth exploring the privacy issues concerning geo-location data under the Fourth Amendment. If the U.S. has a highway surveillance program similar to ETC, it is unclear whether the government is permitted to conduct a warrantless search by requesting that the ETC operator turn over the customer's geo-location data. This article highlights the privacy doctrines previously ruled on by the U.S. Supreme Court and examines whether they are still adequate to respond to new privacy threats posed by new technologies.

*a. Privacy Protection Doctrines under the Fourth Amendment*

The Fourth Amendment of the U.S. Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[110]

The Supreme Court initially interpreted the Fourth Amendment such that to constitute an unreasonable search or seizure under the Fourth Amendment, there had to be physical trespass into private spaces (trespass doctrine).[111] The physical trespass requirement was

---

107. United States v. Jones, 132 S. Ct. 945, 948 (2012).

108. *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 83-86 (2013).

109. See United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

110. U.S. CONST. amend. IV.

111. Olmstead v. United States, 277 U.S. 438, 466 (1928) ("The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment.").

later abandoned in *Katz v. United States,*[112] in which the Court held that:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. However, what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[113]

In his concurring opinion in *Katz*, Justice Harlan set out both the subjective and objective requirements under the Fourth Amendment: "a person have exhibited an actual (subjective) expectation of privacy" and "the expectation be one that society is prepared to recognize as 'reasonable.'"[114] This twofold test laid out the foundation of the widely cited reasonable expectation of privacy test and formed the major consideration when the Court determined the Fourth Amendment claim (reasonable expectation of privacy doctrine). In the time since, the Fourth Amendment protection is no longer limited to physical trespass.

In later decisions when applying the reasonable expectation of privacy test, the Court further formulated another prominent test, the "third-party doctrine," which states, "a person has no expectation of privacy in communications voluntarily provided to a third party."[115] In *United States v. Miller*, the Court held that:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the

---

112. *See* Katz v. United States, 389 U.S. 347, 348 (1967) (holding that "[t]he Government's eavesdropping activities violated the privacy upon which petitioner justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment" and "[b]ecause the Fourth Amendment protects people rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure.").

113. *Id.* at 351.

114. *Id*. at 361 (Harlan, J., concurring) ("As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.' My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.").

115. *See* Allyson Haynes, *Virtual Blinds: Finding Online Privacy in Offline Precedents*, 14 VAND. J. ENT. & TECH. L. 603, 622 (2011).

confidence placed in the third party will not be betrayed.[116]

Under the third-party doctrine, one has no reasonable expectation of privacy in any information that has become known to a third party.[117] The Supreme Court has upheld the third-party doctrine in *Smith v. Maryland*, where the phone numbers a person called were not protected by the Fourth Amendment because the phone company had access to the phone number (reaffirming the third-party doctrine) and because phone numbers are not phone communication content. [118]

Despite the above development when the standards of reasonable expectation of privacy were starting to mature, the Court brought back the trespass doctrine, which was decided inadequate in *Katz*. In *Kyllo v. United States*, the majority opinion written by Justice Scalia cited the trespass doctrine to emphasize the privileged position of the home.[119] Justice Scalia again wrote for the majority in *United States v. Jones* and reaffirmed the position in *Kyllo* that physical intrusion over a property right shall be the leading point to determine Fourth Amendment violation.[120] The *Jones* Court held that "[t]he Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment" because a GPS tracking device on a car is an act equivalent to trespass.[121] In *Jones*, Justice Scalia claimed two types of Fourth Amendment rights. The first was the property right to protect freedom from arbitrary invasions, which was the common law basis in *Kyllo* and is commonly known as the property-based approach.[122] The second is the reasonable expectation of privacy, which was the common law basis in *Katz* and is commonly known as the privacy-based

116. United States v. Miller, 425 U.S. 435, 443 (1976).

117. Gray & Citron, *supra* note 108, at 86 ("[T]he Court has held that the Fourth Amendment cannot save us from 'misplaced confidence' in third parties. Even if we avoid public exposure by only sharing our private activities with a select few, we run the risk that those people will violate our trust by sharing the details with law enforcement.") (footnote omitted).

118. Smith v. Maryland, 442 U.S. 735, 742 (1979).

119. Kyllo v. United States, 533 U.S. 27, 34 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search,' and is presumptively unreasonable without a warrant.").

120. *Jones*, 132 S. Ct. at 949 (2012) ("The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to "the right of the people to be secure against unreasonable searches and seizures"; the phrase "in their persons, houses, papers, and effects" would have been superfluous. Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.") (citation omitted).

121. *Id.* at 946.

122. *See* Devin W. Ness, *Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy as We Know It*, 31 CARDOZO ARTS & ENT. L.J. 925, 939-41 (2012).

approach, applicable in non-physical-invasive monitoring.[123] The *Jones* Court was silent as to whether the traditional third-party doctrine and public observation test exceptions are still suited to the digital age and did not reveal in its opinion how to treat privacy impacts brought by new surveillance technologies such as GPS.[124] Justices Sotomayor criticized, in her concurring opinion, that "[in] cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."[125] Although the *Jones* Court's adoption of the conventional property-based approach to adjudicate the new type technology invasion claim was controversial, it is certain that *Jones* still affirmed *Katz* in the sense that the reasonable expectation of privacy test shall be the leading standard to adjudge the legitimacy of the government's information-gathering, if regarded as non-physical-invasive monitoring.

*b. Are the Fourth Amendment Doctrines still Adequate in the Modern Technology Era?*

Questions have been raised regarding how to apply the classic reasonable expectation of privacy test to disputes caused by emerging technologies[126] because applying a socially recognizable standard of

123. *Jones*, 132 S. Ct. at 953 (2012) ("For unlike the concurrence, which would make *Katz* the exclusive test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.") (citation omitted).

124. Regarding the criticism of the majority's property-based approach, see *Id.* at 961-62 (Alito J., concurring).

125. *Id.* at 955 (Sotomayor J., concurring).

126. *See* Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it*, 72 GEO. WASH. L. REV. 1208, 1201-12 (2003) (Professor Orin S. Kerr indicated that there are three reasons "why it may be difficult under current doctrine for the Fourth Amendment to offer strong privacy protections online." "The first reason is the uncertainty over whether and when Internet users can retain a 'reasonable expectation of privacy' in information sent to network providers, including stored e-mails." The second reason is the Internet makes the Fourth Amendment rules governing grand jury subpoenas weak. According to the third party doctrine, "so long as the third party is in possession of the target's materials, the government may subpoena the materials from the third party without first obtaining a warrant based on probable cause." Therefore, the Government can compel the Internet Service Providers (ISPs) to disclose the information to them without the restriction of Fourth Amendment rules "[b]ecause ISPs are third-party corporate entities." "The third reason that the Fourth Amendment generally offers weak privacy protections online is that most ISPs are private actors. Most are commercial service providers, not government entities. Under the private search doctrine, the Fourth Amendment 'is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'"); *see also* Russell L. Weaver, *Privacy in an Age of Advancing Technology*, 82 MISS. L.J. 975, 992-93 (2013).

reasonable expectation to determine the legitimacy of using new tracking technology is likely to undermine privacy protection. Private information has become more easily accessible by others due to emerging technologies without the data subject's voluntary disclosure. We can depict the dilemma in applying the traditional privacy expectation standard to GPS surveillance as follows: According to *Katz* and *Jones*, to argue for a reasonable expectation of privacy, a person must meet a twofold requirement—a person has exhibited his subjective expectation of privacy and such expectation has to be socially recognizable. If, in the future, society forms a consensus that GPS's main function is to provide a geographic direction service and therefore can be easily used to track the GPS user's location, the objective privacy standard could be interpreted in the manner that one has less expectation of privacy when using GPS devices. Some favoring this position might add that stalking by machine does not present greater invasion to one's privacy because GPS surveillance only electronically monitors the vehicle, not directly watch the movements of the targeted person, and what is being watched through GPS surveillance is the car's movement, not the human being. However, can this argument (i.e., the GPS tracing device is less invasive than a stalker) hold true in other situations where other variables are involved? For instance, if the GPS device is used by the police to monitor the suspect's whereabouts for an entire month, compared to the situation where the police deploy a team of investigators to follow a suspect for just one day, which scenario poses a more severe privacy threat? The line does not seem to be clear.[127] It would be very difficult for one to invoke their Fourth Amendment right if their claimed expectation of privacy is not supported by the society's norms and standards.

(1) Problematic Third-Party Doctrine for Digital Privacy

The Court in *Miller* originally established the third-party doctrine to supplement the "reasonable expectation of privacy test" in *Katz*. The principle is that a person generally has a reasonable expectation of privacy in private information, but if a person puts the information into the hands of someone else, the person's privacy interest is not protected by the Fourth Amendment because we know of the risk that a "third party" will share the information with others.[128] As soon as the information is uploaded to the Internet, the individual must necessarily anticipate that the personal information will become generally visible to others, and thus, the third party doctrine will render the data ineligible

127. *See* Gray & Citron, *supra* note 108, at 83-100.
128. United States v. Miller, 425 U.S. 435, 435-36 (1976).

for Fourth Amendment protection.[129] The result of applying the third-party doctrine is problematic because one's posted activities on online social networks are not treated as information with a reasonable expectation of privacy even if the account is set only for friends due to the application of the third-party doctrine.[130]

The third-party doctrine faces challenges in regard to information privacy issues arising from the use of modern technologies such as e-mail, whether this doctrine is adequate to apply to e-mails remains to be tested in courts. A notable opinion by the Sixth Circuit Court of Appeals' has revised the third-party doctrine held by the Supreme Court. In the *United States v. Warshak*, an e-mail user argued that "the government's warrantless, ex parte seizure of approximately 27,000 of his private emails constituted a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures." [131] The Sixth Circuit court held that the e-mails stored by e-mail service providers are protected by the Fourth Amendment; the government needs a search warrant based on probable cause to seize e-mail messages.[132] However, the court wrote an arguable sentence that may open the door for e-mail service providers to lessen their data protection obligation: "if the ISP expresses an intention to audit, inspect, and monitor its subscriber's emails, that might be enough to render an

---

129. *See* Haynes, *supra* note 115, at 628-29 (indicating that in the online context, if we apply the law strictly, "there is by definition no right of privacy on the Internet, either because it is seen as 'public' and not 'private,' or because communicating via the Internet necessitates sharing with a third party.").

130. *See* Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 656 (N.Y. Sup. Ct. 2010) ("Indeed, as neither Facebook nor MySpace guarantee complete privacy, Plaintiff has no legitimate reasonable expectation of privacy. In this regard, MySpace warns users not to forget that their profiles and MySpace forums are public spaces, and Facebook's privacy policy set forth, inter alia, that '[y]ou post User Content . . . . on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable.' Thus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, '[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.'") (citation omitted); *but see* Haynes, *supra* note 115, at 645 (Professor Allyson W. Haynes criticized the court decision and indicated that "[t]he court failed to give any weight to the plaintiffs affirmative action in restricting her disclosures via hei privacy settings. To the court, disclosure on an OSN was equivalent to public disclosure, regardless of her efforts to limit her audience. This traditional view of privacy as secrecy fails to recognize any right to control the extent of that disclosure.") (footnote omitted).

131. United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

132. *Id*. at 274.

expectation of privacy unreasonable."[133]

In addition to *Warshak*, a number of email users have taken the initiative to challenge email service providers' scanning their emails. The Internet giant and email service provider, Google, is being sued for violation of privacy by scanning the contents of Gmail messages in order to capture information about its users and to send advertisements.[134] This case is in its preliminary stages and it might be too soon to tell how the court will rule on the dispute. Nevertheless, if the presiding judge decides to allow for a potential class-action suit against Google and rejects Google's arguments that users have no expectation that their e-mail communications will not be read by e-mail service providers,[135] the court may have signaled that the third-party doctrine presented in *Miller* in an offline world needs to be reconsidered. It is worth noting that when Google argued that all Gmail users must expect that their e-mails will be subject to automated processing, the court noted that Google's privacy policy did not specify whether Google is scanning the content of the e-mails.[136] However, even if Google's Gmail privacy policy expressly stated that it monitors subscriber's e-mail content, which *Warshak* notes as an exception to the reasonable expectation doctrine, is it reasonable to jump to the conclusion that Gmail users would no longer have any reasonable expectation of privacy regarding their private e-mail communications? The time has come to reexamine the third-party doctrine in the digital age.

To many email users, the role of an e-mail service provider is no different from that of the post office in helping to deliver private communications, irrespective of whether the form of transmission is in print or online. In the offline world, when one mails a letter to a friend, by applying the *Miller* test, it seems reasonable that one cannot claim a reasonable privacy expectation in a letter because one should perceive the risk of the letter being disclosed to the public as soon as the letter is out of the sender's control. It should be noted that even when applying the third-party doctrine, the third party is the intended addressee of the letter. The third-party doctrine does not imply exemption of the post office from the obligation to respect the sender's privacy and to protect the letter from prying. The post office should not be the third party

133. *Id.* at 287.

134. *See* Hayley Tsukayama, *Judge Allows Lawsuit against Google's Gmail Scans to Move Forward*, WASH. POST (Sept. 26, 2013), http://www.washingtonpost.com/business/technology/judge-allows-lawsuit-against-googles-gmail-scans-to-move-forward/2013/09/26/3b4bedaa-26e4-11e3-b75d-5b7f66349852_story.html.

135. *Id.*

136. *Id.*

under the privacy exception.

Unlike the post office, e-mail service providers may claim to be the third party under the *Miller* test. Post office or mail carriers do not need (and are not allowed) to *open* a sealed *envelope* in the course of delivery, whereas electronic e-mails will be subject to automated processing by ISPs and email providers. For e-mails, not only can the receiver read the message, but every word in the e-mail is also open and visible to email operators and others who have access to the system, even if the contemplated receiver does not open the e-mail at all. If e-mail users must expect that their e-mails will be read by the service provider because this is how electronic mail techniques work, e-mail service providers may claim to be a third party under the third-party test. However, is society prepared to recognize that private e-mail messages are not subject to Fourth Amendment protection by applying the third-party test?

The above discussion underscores the fact that the earlier adopted "reasonable expectation of privacy test" does not respond well to the privacy invasion concerns arising from new information technologies, and failure to modernize the non-digital world standard to adapt to technology changes will threaten privacy protection. The "objective reasonable expectation standard" *is* intended to examine whether society is prepared to recognize the privacy expectation as reasonable. Technological progress can affect society's expectation of information privacy and shift the line of this objective standard. When private information becomes more easily accessible by others due to increasing use of modern technologies, it also becomes more difficult for the data subject to claim a reasonable expectation of privacy in the piece of personal information.[137]

(2) New Technology Blurs the Line between Content and Non-content Information: Phone Numbers vs. IP Addresses

In *Smith*, the United States Supreme Court held that the phone numbers a person called were not protected by the Fourth Amendment, partly in because the phone numbers were not phone communication content.[138] Some call this the "content-envelope distinction" standard.[139] The content information is the letter itself and the envelope information is the address.[140] According to this standard, the Fourth Amendment does not protect phone numbers dialed or the addresses of letters sent

137. *See* Weaver, *supra* note 126.

138. Smith v. Maryland, 442 U.S. 735, 742 (1979).

139. *See* DANIEL J SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 157 (2011).

140. *Id.*

because envelope information is less sensitive than content information.[141] Similar to telephone numbers, which are used by telephone companies to complete the call, an IP address is a set of numbers assigned to every computer when users log onto the Internet.[142] By applying this test, an IP address is necessary for ISPs to complete the service and does not involve the merits of communication, so an IP address does not seem to be protected by the Fourth Amendment.[143] Some have questioned whether IP addresses are just numbers without any content. IP addresses have distinguishable features that phone numbers do not have—an IP address can show a map of how a person surfs the Internet.[144] When an IP address can indicate a person's surfing activities on the Internet, leading to disclosure of the subject's consumption habits, health condition and personal interests, whether the content/envelope distinction test still applies needs to be considered.

Phone contacts, the length of a telephone conversation, and where the phone conversation took place, when viewed individually, may not have a direct connection with phone content. However, when different pieces of contact information are integrated, they can generate profiles about the behavior of specific persons. For instance, a combination of location data and mobile phone communication records can reveal details of secret meetings or conversations between politicians and lobbyists. In other words, sophisticated technologies have challenged the content/envelope distinction test, requiring it be revised. *As* Justice

---

141. *Id*. "Congress embodied [content-envelope distinction] in the law. Content information is regulated by the Wiretap Act and the Stored Communication Act, and it is given high-level privacy protection. Envelope information is protected by the Pen Register Act, which provides low-level privacy protection." *Id*.

142. *Id.* at 158; *see also* Stephanie Crawford, *What is an IP address?*, HOWSTUFFWORKS, http://computer.howstuffworks.com/internet/basics/question549.htm (last visited Feb. 23, 2014) ("Every machine on a network has a unique identifier. Just as you would address a letter to send in the mail, computers use the unique identifier to send data to specific computers on a network. Most networks today, including all computers on the Internet, use the TCP/IP protocol as the standard for how to communicate on the network. In the TCP/IP protocol, the unique identifier for a computer is called its IP address.").

143. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("[T]he surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*. First, e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").

144. *See* SOLOVE, *supra* note 139, at 158-59.

Louis Brandeis claims, the Fourth Amendment must have a "capacity [for] adaptation to a changing world."[145] Social network operator, Facebook, has identified in its policy of Information for Law Enforcement Authorities that location information constitutes content information:

> A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.[146]

Recent legislative activity in Taiwan has proposed the strengthening of privacy protection on traditionally non-content private communications.[147] A few months before the outcry over the United States Senate Intelligence Committee on the United States Central Intelligence Agency's accused spying activities,[148] a similar dispute occurred in Taiwan, stemming from the Taiwanese intelligence agency's surveillance of the president of the Legislative Yuan, Taiwan's parliament, and a number of opposing party parliament members.[149] This event led to a proposition to amend the Telecommunications Act to impose a requirement that investigators and prosecutors obtain a judicial-granted order before spying on individuals' dialed and called telephone lines, the names of persons called, the length of the phone conversation, and all other non-content communication records. This proposed amendment represents the reaction to privacy challenges under new technologies and the need to extend privacy protection to areas that were traditionally regarded as merely a format not involving content.

---

145. Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting).

146. *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines/ (last visited July 28, 2014); *see also* NATE CARDOZO, ET AL., WHO HAS YOUR BACK? WHICH COMPANIES HELP PROTECT YOUR DATA FROM THE GOVERNMENT?, THE ELECTRONIC FRONTIER FOUNDATION'S THIRD ANNUAL REPORT ON ONLINE SERVICE PROVIDERS' PRIVACY AND TRANSPARENCY PRACTICES REGARDING GOVERNMENT ACCESS TO USER DATA 9 (2013), *available at* https://www.eff.org/sites/default/files/who-has-your-back-2013-report-20130513.pdf.

147. *See* 吳景欽 [Wu Jing Qin], *非關犯罪之通聯紀錄調取之疑義* [*Issues of Accessing to Personal Communication Records for Purposes Not Related to Criminal Investigation*], 今日新聞網 [NOWNEWS.COM] (Jan. 24, 2014), http://www.ettoday.net/news/20140121/318115.htm.

148. *See* Adam Serwer, *Senator Accuses CIA of Spying on Congress*, MSNBC (Mar. 11, 2014, 10:16 AM), http://www.msnbc.com/msnbc/feinstein-cia-senate.

149. *See* 賴又嘉 [Lai You Jia], *特偵控關說　柯建銘監聽譯文全文* [*The Special Investigation Crew Accused Ko-Chien-Ming of Engaging in Illegal Lobby; A Full Transcript of Ko's Conversation*], 蘋果日報 [APPLE DAILY] (Sept. 6, 2013), http://www.appledaily.com.tw/realtimenews/article/new/20130906/254624/.

*c. Is Geo-location Data Protected under the Fourth Amendment?*

In *Jones*, the Court decided privacy intrusions occurred due to the police's physical attachment of a GPS device to a car without a search warrant but left the question unanswered as to whether the police surveillance was made without physical attachment of the GPS device.[150] After all, the real question is whether surveillance in public and access to records held by a third party constitutes privacy invasion protected by the Fourth Amendment; the type of devices used for the surveillance should not affect the answer. *Jones* also by no means suggests that had the police used a non-physically-attached device the warrantless surveillance would have been legitimate. Before the Supreme Court addresses this troubling issue, we must examine where geo-location data falls on the spectrum of the above-mentioned privacy doctrines.

It is true that geo-location data generated by GPS, mobile devices (such as smartphones and tablet computers), and the ETC system merely indicate the location of the devices and do not directly reveal the identity of a person. However, similar to an IP address, which has the important feature of indicating the device user's behaviors on the Internet, geo-location data can also be easily linked to a specific person who carries the device to track his location and movements, a new category of personal information that did not exist before such devices were available. The question is whether the "location" or "movement" shall be reviewed as content or non-content information, as the Supreme Court has excluded non-content information from the Fourth Amendment protection due to the less-personal-sensitive nature. Geo-location data is not just the data of the tracked devices but also that of the specific individual and that data can disclose a person's social activities and other livelihood information, which concerns one's private and family life.[151] Therefore, geo-location data should not be treated the same as envelope information in terms of privacy protection.

One may argue that geo-location data concerns one's public activities, and when one exposes himself to public observation, he cannot claim a reasonable expectation of privacy. However, one's expectation of being watched and having every movement recorded are two different things. Walking or driving in a public place is not equivalent to the relinquishment of privacy entirely. One may realize that other people in public venues can see his movement. There are speed cameras deployed along the roads to detect and deter speeders and red light runners. Nonetheless, this expectation is far from being

150. *See* United States v. Jones, 132 S. Ct. 945, 948 (2012).

151. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 702-16 (2011).

put into a surveillance web through data from GPS, cell towers, or the ETC system. Unless it has become acceptable by society for video cameras or other surveillance devices to be set up in public places to capture citizens' every movement, according to *Katz*, we cannot assume that there is no reasonable expectation of privacy vested in these geo-location data. Moreover, although the geo-location data is available to mobile phone companies, GPS, or ETC operators, according to *Warshak,* this does not mean that device users necessarily lose their reasonable expectation of privacy under the Fourth Amendment, and the government may still need a search warrant based on probable cause to seize the geo-location data.[152] Of course, different scenarios involve various factors of the conflicts between personal privacy and the needs of criminal investigation or other purposes, and the solution remains to be answered by the Court.

### F. GOVERNMENT'S ROLE IN PROTECTING ETC PERSONAL DATA

The above conclusion, that the CIB has no statutory grounds to request FE-Toll to turn over the E-Toll data is supported by the privacy right's negative (or defensive) function against the government's intrusion. In fact, the constitutional right to information privacy carries a positive dimension, under which the government has an affirmative obligation to take action to protect people's information privacy.[153] In a dispute concerning a conflict between the right to privacy and the right of free press, Taiwan's Constitutional Court has reaffirmed the constitutional right to information privacy and declared that the government has an obligation to safeguard such right, even though the infringement of privacy is not from the government but from the private sector.[154] Following this notion, in situations where private

152. *Id*. at 742-43 ("Under a reasonable expectation of privacy analysis, location data implicates the Fourth Amendment, and its acquisition by law enforcement should proceed only after agents obtain a warrant based on probable cause.").

153. *See* Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 HARV. J.L. & PUB. POL'Y 605, 622–23 (2013) ("The EU Data Protection Directive requires each member state to establish a public authority responsible for 'monitoring the application within its territory of the provisions adopted' . . . . Data protection authorities have an affirmative obligation to determine which processing operations are likely to present specific risks to the rights and freedoms of data subjects and examine them before they are commenced.").

154. *See* J.Y. Interp. No. 689, at reasoning ¶ 6 (July 29, 2011) (Taiwan), *translated in http://jirs.judicial.gov.tw/eng/FINT/FINTQRY03.asp?Y1=2011&M1=&D1=&Y2=&M2=&D2=&cno=&kw=&btnSubmit=Search&sdate=20110000&edate=99991231&keyword=&page=3&total=35&seq=30* ("[T]he liberty to be free from intrusion in the public sphere can only be asserted when it can be reasonably expected; that is, the expectation of non-intrusion must not only be manifested but also deemed reasonable by the general public. The Provision at issue has met the constitutional requirement of the State to guarantee the aforementioned rights and liberties.").

companies take the initiative to voluntarily sell personal data to public agencies, the latter is prohibited under the Taiwan Constitution to buy such data if the disclosure is not authorized by the data subject or by other laws.[155] Furthermore, when the Taiwan's National Freeway Bureau (NFB) contracted FE-Toll to operate the ETC system, the NFB had a constitutional obligation to carefully evaluate the privacy implications when a conglomerate controls the entire nations' driver data, or at least the government should find ways to avoid or mitigate the negative privacy implications. Failure to perform the privacy safeguarding obligation constitutes a violation of the duty of the respective agency to safeguard people's interest in information privacy.

The government does not seem to have fulfilled the affirmative obligation to protect the right to privacy by allowing FE-Toll and its shareholder to control drivers' data regarding the use of highways and all major roads in the entire nation without limitation. FE-Toll's major shareholder, Far EasTone Telecommunications Co. Ltd. (FET), is one of the major providers in Taiwan's mobile service market and has recently been selected by the Ministry of Transportation and Communications to construct and operate the Integrated Traffic Service Cloud project (December, 2013).[156] The Traffic Cloud is intended to integrate all traffic information gathered by all road agencies across Taiwan and to systematically analyze the traffic information in order to provide real time traffic and travel information and alerts to citizens.[157] By winning the bid to undertake the Traffic Cloud project, FET can control all information gathered through roadway surveillance and traffic cameras originally collected and managed by the respective public sectors. FET also has access to public transportation networks including metro, bus, and train travel across cities and counties. In addition to officially taking over public sector information, FET may also exercise its right as a contractor of the Traffic Cloud to install traffic cameras on all city and county roads to conduct surveillance on all vehicles 24 hours a day, 365 days a year.[158] FE-Toll and FET together will control nearly one hundred percent of the traffic surveillance data of all major levels of roads across the country.[159]

With the government controls the drivers' data, there are already fears of inadequate processing of personal data because the implementation of privacy laws cannot provide full assurance that no

---

155. *Id.*

156. *See* 朱致宜 [Zhu Zhi Yi], *個資看透透　徐旭東變「全民公敵」？* [*Surveillance of Personal Data Shu-Shu-Dong Becomes All Citizens' Enemy?*], 財訊 [WEALTH MAG.] (Jan. 15, 2014), https://www.wealth.com.tw/index2.aspx?f=301&id=3915.

157. *Id.*

158. *Id.*

159. *Id.*

breach of security will occur. The government's outsourcing of the management of said data has made personal data more vulnerable because the laws limiting the government's use of personal data is not applicable to private sectors.[160] The relationship between private data controller and data subject will mostly be decided by contracts (such as ETC user contracts). In reality, whether individuals can obtain sufficient and genuine privacy protection from these contracts is highly doubtful when businesses' bargaining power is far greater than the individual customers.

Putting aside FET's Integrated Traffic Service Cloud project and only focusing on the ETC program, the government is not doing enough to safeguard people's right to information privacy. After the implementation of the ETC system, the national highway toll system has completely converted to e-toll lanes, and all manual fee payment routes have been removed. This policy is tantamount to forcing all highway users to accept monitoring by the ETC. The policy makers have failed to consider whether there is an inequality in the bargaining position between FE-Toll and highway drivers because FE-Toll controls the highway entrance and citizens will be denied access to the highways if they do not accept the terms of the conditions set by FE-Toll. In such a situation, the government has a constitutional obligation to step in and scrutinize the one-sided contract to protect people's privacy and require FE-Toll to implement and maintain adequate measures for confidentiality and security to protect personal privacy. Unfortunately, at the time of writing, the government does not seem to have fulfilled such obligations.

The Internet combined with mobile devices has formed a pervasive surveillance net, and it is nearly impossible to escape from it. Businesses have greater capabilities to track, maintain, and analyze data to profile digital dossiers of individuals (digital persons).[161] The

---

160. *See* Personal Information Protection Act art. 15, 19. The PDPA distinguishes public and private sectors when setting out rules for the sectors' collection, process and use of personal data. For example, Article 15 of the PDPA applies to government agencies to regulate their actions related to data collection and use, whereas Article 19 apples to private sectors' collection and use of personal data. *Id*.

161. "Digital person" concept is introduced by Professor Daniel J. Solove. In his book, *The Digital Person*, he indicates that:

> [d]igital technology enables the preservation of the minutia of our everyday comings and goings, of our likes and dislikes, of who are and what we own. It is ever more possible to create an electronic collage that covers much of a person's life—a life captured in records, a digital person composed in the collective computer networks of the world.

DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1 (2004).

new information technology allows the linkage of geo-location data with identity, significantly reducing the possibility for individuals to be left alone.[162] Individual choice is no longer a valid form of privacy protection. The ETC case is the perfect real life example to illustrate the challenges to information privacy under the widespread use of advanced technology. The launch of ETC has forced all drivers to use electronic toll collection lanes and deprived people of their privacy rights if they decide to use the national highway system. It is essential that there be specific and articulated grounds to force people to give up their privacy to use the highways, and these grounds should meet the requirement of necessity and the principle of proportionality. The government should not be in a role to abet a conglomerate in obtaining personal data to expand its business territory without giving the individual a choice over his personal information, which constitutes a violation of the duty of the government stipulated in Article 22 of the Taiwanese Constitution.[163] If there is a compelling public interest behind the sweeping collection of people's vehicle data, due to the government's obligation to protect people's information privacy under the Constitution, the government should actively supervise the formation of the ETC users' contractual clauses instead of allowing FE-Toll to unilaterally decide the terms and conditions. Furthermore, it should impose obligations on FE-Toll to implement and maintain adequate controls of the E-Toll data's security, and it should require FE-Toll's full cooperation with regulatory investigations and audits for ongoing privacy protection assurance.

## IV. CONCLUSION

Information technology is moving forward at full speed. The same day the author finished the final draft of this article, Facebook unveiled a new innovation, "Nearby Friends," which allows its users to track their friends' location in real time.[164] With this feature, Facebook users now share more details about their geo-location data. We have to realize that the pace of law making can never equal the pace of technology advances. Seeking to craft laws for information privacy protection following every move of technology innovation is a long shot and is likely to miss the target. As fast and diverse as technologies can

---

162. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("the right to life has come to mean the right to enjoy life,- the right to be let alone.").

163. Article 22 of Taiwanese Constitution provides that "All other freedoms and rights of the people that are not detrimental to social order or public welfare shall be guaranteed under the Constitution." Minguo Xianfa art. 22 (1947) (Taiwan), *available at* http://db.lawbank.com.tw/Eng/FLAW/FLAWDAT01.asp?lsid=FL000001.

164. *See* Tsukayama, *supra* note 134.

be, it is vital to reconsider the core value of privacy in the rapidly changing technology era and to clarify the concept of information privacy in a way that it can withstand technology innovations.

United States privacy legislation is sector-centered and does not have a single omnibus information privacy protection law. There are fragmented statutory protections for selected types of personal information, such as financial privacy, educational records, health data, telecommunications and marketing, online privacy and workplace privacy. Geo-location data does not seem to be regulated under these categories. The current U.S. information privacy law has gaps regarding geo-location data protection. For example, if United States government agencies want to adopt a similar bulk vehicle data surveillance program to collect geo-location data or to seek access to geo-location data if they are collected by companies, there will be at least two issues regarding the applicability of the Fourth Amendment: whether geo-location data concerns the content of personal communication and shall receive higher protection than envelope information and how to treat geo-location data under the third-party doctrine. Whether Fourth Amendment protection will be afforded to individuals concerning geo-location data is still unknown. Lacking a comprehensive law, data subjects will have to address the variety of privacy laws to seek protection, especially for the new type of information. A common criticism is that gaps can occur in the fragmental approach and that unregulated segments will face privacy threats when legislation lags behind technological innovations.

As a comparative law perspective, the Taiwanese information privacy law approach to adopt a comprehensive privacy protection model could be an option for United States information privacy reform to better protect information privacy. Of course, the comprehensive privacy law approach has its own disadvantages, and there are debates in Taiwan about whether the government's access of geo-location data requires search warrants. The level of strictness of legal instruments depends on the legal risk nations are willing to accept, which is not the focus of this essay. Nonetheless, an omnibus model ensures a basic level of privacy protection for most data and serves to prevent gaps in privacy protection for new data yielded by new technologies. For companies that wish to lawfully collect and use data, a comprehensive standard sets the line of personal information gathering and use, especially when new devices are involved. Another immediate benefit is that when the government is making requests to companies to turn over customers' information, companies have a legal basis to decide whether to comply with such requests, especially when some agencies attempt to evade their compliance obligation in direct information gathering from the data subject and instead requesting that companies turn over data.

Enterprises are driven by potential business opportunities to upgrade technologies to facilitate data collection and analysis, and they appear to possess more personal data than government does. For individuals, such an omnibus privacy law can offer certain protection against privacy invasions by giant corporations'.