# Some Thoughts about the Past, Present, and Future of the Right to Information Privacy in Taiwan

Ching-Yi Liu
(J.S.D. The University of Chicago Law School;
Professor of Law, National Taiwan University)

October, 2018

Professor Ting-Chi Liu is one of the leading experts in Taiwan's information privacy law. His paper on the development of the right to information privacy from a comparative law perspective does provide us with some useful guidance for our understanding on the conceptual history of right to privacy information and the current challenges it faces for the past few years. Viewed from this perspective, Professor Liu's observations and suggestions about the future of the right to information privacy can serve as a nice roadmap as to how we in Taiwan can adequately protect the right to information privacy while harnessing the potential benefits of modern information technology at the same time. As I have the privilege of reading Professor Liu's paper in advance, I would like to share with Professor Liu and the other participants of this panel about my comments and questions on the issues related to Taiwan's information privacy law. And I believe this is a great opportunity for our exchange of ideas and I can learn a lot more from you.

**A. The Privacy Perils of Open Data Policy**

The past decade has witnessed a wave of open data initiatives. More and more governments and corporations have embraced the idea of open data and have released the raw data sets to the public that used to be collected, stored and buried deep in their own databases. While open data initiatives are seen as rendering government records more accessible to the public, encouraging technological innovation and economic development, motivating civic engagement, they also received some criticism focusing on the questions as to whether the use of data is appropriate and whether just one reckless act could cost data subjects' privacy interests. In my sense, it goes without saying that privacy should be in the center of debates when making open data policies. A comprehensive data protection program is the key to the fulfillment of the promises that the open data advocators have pictured. I would love to learn more about Professor Liu's observations on the case of Taiwan's open data policies/initiatives, especially how he will evaluate these policies/initiatives under the regulatory context of GDPR.

**B. The Protection of Sensitive Personal Data**

It seems to me that Professor Liu's observations on our information privacy law focus on the struggle between the "old laws" and the "new technologies." However, I would like to say that the following major flaws in Taiwan's Personal Data Protection Act (PDPA) are the origin

of the struggle. First of all, the insufficient protection of sensitive personal data is the key controversy in PDPA and it gave rise to the dilemma we have today. In other words, as Article 6 of the PDPA that required stronger protection toward "sensitive personal data" and other strict regulations were met by oppositions from private sectors for the reason that "it would cause tremendous hardships for corporations to abide by the law," eventually this contentious Article and Articles related to its enforcement had been suspended and led to another round of amendment of the PDPA in 2015.

The Ministry of Justice claimed that the purpose of the amendment to the PIPA in 2015 was to make the law to "keep up with the current social circumstances". For instance, under the 2015 PIPA, except for under the situations of collecting sensitive data, data collectors no longer need to obtain "written consents" from data subjects. In other words, a simple "consent", even an implicit one, will meet the requirement. The Ministry of Justice, which proposed the amendment, reasoned that relaxing the requirements of consent could ease administrative burdens from government agencies and save costs for private sectors. But the civil society criticized that this clause along with many other amendments actually trade individuals' information privacy for the conveniences and benefits of data collectors and processors. In the context of open data in which the protection mechanism of individuals' information privacy, such as de-identification and informed consents, should be taken into serious consideration, the newly amended PDPA not only falls short of closing the loopholes of the law, but also increased risks of privacy violations.

**C. Why De-identification?**

As Professor Liu has mentioned the NHIA case, it seems necessary to talk about the de-identification controversy. Although the purpose of the PDPA is to protect personal information, the law has only addressed the issue of de-identification in a very general way. For instance, is the de-identification strong enough if the data subject could not be identified at the first glance of the information? Or the de-identification should be irreversible that the data subjects cannot be identified even when the data is combined with other data sets? Neither does the PDPA provide sophisticated requirements of de-identification for different kinds of data and in various contexts of data reuses.

As a matter of fact, both the NHIA case and the ETC case reveal that the ambiguity about the de-identification in the PAPA has allowed the data collectors and processors certain leeway when they conduct de-identification to meet the current legal requirement. It is completely predictable that for the sake of convenience and saving costs, the collectors and processors have chosen relatively easy ways of de-identification. However, the weak de-identification has led to perils of exposing the identities of data subjects. Also, another issue concerns de-identification in the PIPA is the obscurity of who should bear the responsibility of de-identification. The provisions in the PDPA involving de-identification states that "[t]he information may not lead to the identification of a specific person after its processing by the provider, or from the disclosure by the collector." In other words, it could be the data providers or the collectors who de-identify the data. The ambiguity of the responsibility could result in that both providers and collectors shed burdens of de-identification and bring about more disputes. Moreover, due to the uncertainty of who should de-identify the data, the time of data to be de-identified could be delayed, which means that there could be more risks of information privacy violation against the data subjects.

**D. The Right to Consent and Opt-out**

"Informed consent" is an important mechanism for individuals to control the flow of their own information. The amendment to the PIPA in 2010 thus required the data collectors to obtain written consents from data subjects under general circumstances. However, to ease the burden from data collectors, especially in the situation where the volume of the data is large, the newly amended PIPA in 2015 lifted the requirement for written consents except for collecting sensitive personal information. Now when dealing with non-sensitive personal information, the data collectors or providers do not need to obtain "written consents"; only "consent" will suffice.

According to the PDPA, even in the circumstances where sensitive data is involved, consents from data subjects is not a necessary condition for data collectors or providers to collect or use data. Furthermore, other conditions, such as for the purpose of public interest in academic research, or assisting government agencies to carry on their duties, are listed in the PDPA as justifications for data collectors or providers not to obtain consents. From collectors' point of view it seems apparent that the newly amended PDPA has solved the hurdle of obtaining consents when a large number of data subjects are involved, such as in the situation of open data. But for data subjects, that means they lose the right to refuse their own data being used without clear consent.

What is even worse, the PIPA doesn't give data subjects the right to ask data collectors or providers to stop using their personal information, either. Although the PIPA has provided that data subjects have the rights to request their information to be "deleted, discontinued to process or use" when "the specific purpose no longer exist or time period expires", data subjects still cannot choose to "opt-out" the databases or the programs once they find out their rights to privacy have been violated or face the risks of being exposed of their identities. Neither does the court support the "opt-out" right. As the NHIA decision reveals, the Supreme Administrative Court in Taiwan still ruled in favor for data collectors and stated that "public interest" trump individuals' right to their information privacy.

**E. The Ambiguity of "Public Interest" in Taiwan's Information Privacy Law**

The term "public interest" has appeared repeatedly in the PDPA and has served as an exception for data collectors or providers to be exempted from certain legal obligations. For example, Article 16 of the PDPA allows government agencies to use data for purposes other than the original ones. For instance, In the ETC case, the Freeway Bureau has apparently applied this exemption to the ETC data system. It claimed there are public interest justifications in opening up the data to the public, and thus the Bureau could use the data that was collected and processed originally for collecting freeway tolls, and even under the circumstances without obtaining consents from data subjects. The controversies caused by the term of "public interest" in regulations are its vagueness, and the danger of overexpansion of its application to the situations that may endanger data subjects' information privacy. Under Taiwan's historical and social context in which the government has had a long history of using the excuses of "maintaining social order" and "promoting administrative efficiency" in policing its people, the risk of excessive uses of "public interest" by data collectors or processors are even higher. As a matter of fact, the government and the court have inclined to assume the requirement of public interest has been met if a program is carried out for public

purposes in public sector, such as open data cases. But the data users (in most cases, the government) and the court have never done any careful or meticulous analysis to look into what the public interest at issue is, nor have them weigh the importance of public interest against individual's right to privacy. Under this situation, those who employ public interest justifications usually prevail and individuals' privacy interests are usually setback.

**F. Revamping Our Privacy Law for the Protection of Information Privacy**

I believe a set of sophisticated data protection regulations is the bedrock of a robust information privacy protection framework and the key to a successful open data program. There are several issues that needed to be addressed in the current data protection regulations in Taiwan: the inadequate requirements for consents that save the works for data controllers and processors but fail to protect data subjects, the lack of "opt-out" device for data subjects, obscured de-identification requirements, and the vagueness of the term "public interest" stipulated in the law.

To guarantee the data subjects' right to information privacy, some ideal amendments to the PDPA would be indispensable as they can help clarify the responsibility of de-identification between the data controllers and processors, offer more sophisticated regulations of de-identification and consent requirements for different kinds of data sets, and demand more comprehensive rationales when government agencies or private companies evaluate "public interests" against individuals' right to privacy.

When it comes to de-identification, some regions or countries have adopted regulations that offer multiple options to de-identify data. For example, GDPR implicitly categorizes different kinds of data, such as identified and identifiable ones, and demands for different levels of de-identification for each category of data. Similarly, in United States, Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule also sets rationales, related standard and two different paths of de-identification for healthcare providers or those who deal with personal health information to follow. After complying with the regulations to reduce privacy risks, the data controllers or users could make the secondary use of the sensitive data.

As for the balance between public interest and individual privacy, it is never easy to make the decision on which one should prevail. It is obvious that Taiwan is not the only country struggling with the definition and scope of the term "public interest," but some other countries or jurisdictions that are faced with the same issue have made efforts to set rationales, or lay down more stringent privacy protection mechanisms into regulations as complementary measures. For instance, in GDPR, the law also allows data controllers and processors to use personal data for the purposes that are beyond the original one without obtaining consents from the data subjects, if the purpose is for public interests such as "statistical purposes or scientific research." However, the GDPR also asks member states to define what "public interests" is, and imposes more detailed requirements for data safeguard. Besides, the sophisticated requirements for data de-identification shall serves as another safe net for data subjects under the circumstances where public interests trump individuals' right to privacy.

To sum up, I agree with Professor Liu that Taiwan should strive to find a suitable approach that can effectively protect individuals' rights to information privacy while allowing the people to harness the potential benefits of advancements in information technology. However,

information technology would cause hazards if it is carried out without thorough plans for privacy protection. A good privacy protection plan would require the mindset that recognizes the important of information privacy, a robust framework for the protection of information, and comprehensive legal mechanisms. To keep the momentum of information technology going in a more balanced way, the strengthening of information privacy protection would be an urgent must-do for Taiwan.

# 關於臺灣資訊隱私權的一些看法

劉靜怡
（國立臺灣大學教授）

## 中文摘要

本人針對論文發表人劉定基教授的主張提出評論意見。基本上，劉教授對於資訊隱私權的比較法觀察均屬正確，因此，本人乃針對劉教授的觀察提出一些補充觀點。首先，本人針對臺灣目前的開放資料政策，在資訊隱私保護的配套措施上是否有需要改進之處，提出質疑。其次，本人針對目前臺灣在資訊隱私權保護上所遭遇到的「敏感性個人資料」「去識別化」「告知後同意與選擇退出的權利」和「公共利益的模糊性」等爭議，提出個人看法，最後則以資訊科技時代應有怎樣的資訊隱私法制，才能讓科技發展與隱私保護兩者以衡平的模式並行不悖，作為結論。