Taiwan's PIPA: One year on

Increasing number of complaints by individuals emerge. By **Chen Hui-ling**.

Taiwan's Personal Information Privacy Act (PIPA) took effect on 10 October 2012. This article reviews incidents in which major corporations inadvertently disclosed personal information, reports a few typical decided cases, and closes with some observations on the wider implications of the PIPA and administrative developments one year on.

Corporate Disclosures

Far Eastern International Bank: In November 2012, large numbers of sensitive documents belonging to Far Eastern International Bank were discovered intact in a recycling plant. The discovered documents included customer passbooks, employee cards, and photocopies of national ID cards. Although this incident was widely publicized in Taiwan's traditional and social media, neither the customers nor the authorities have taken any public action.

Nokia Taiwan: In February 2013, Nokia disclosed that its Taiwanese subsidiary's websites had been hacked and about 1.5 million personal files compromised, including 170,000 records of personal data collected from consumers. The PIPA provides that individuals can claim compensation ranging from 500 NTD to 20,000 NTD (c. US$17-$680) in such cases. Nokia was therefore exposed to a potential maximum statutory claim of NT$200 million (c. US$6.8 million). Again, the extent of the leaks and the amount at stake attracted wide media attention; however, despite calls for rigorous investigations by the authorities, there have been no further public developments. Likewise, no consumers have brought claims to date.

Decided Cases: Individual Disclosures

Despite the lack of PIPA-related enforcement or litigation against corporations, one significant development has been the small but increasing number of claims against individuals. Under the pre-PIPA regime, only the so-called "Eight Major Industries" were subject to personal data protection law. The regulated industries included telecommunications, financial services, media, and health but not natural persons. The advent of the PIPA not only made the personal data protection law's enhanced protections applicable to natural persons, but also gave them standing to seek redress. The cases below deal in the most part with natural persons who imprudently violated provisions of PIPA and therefore exposed themselves to civil or criminal liability.

Civil cases

(102) Fengjian Zi No. 164 (Taichung District Court, 2013): In one of a number of cases arising from disputes at housing complexes, the chairman of the management committee of a housing complex located in Taichung City's Fongyuan District posted court documents from a lawsuit against the previous chairman and vice-chairman of the committee on a physical community bulletin board. The documents contained personal information such as birth dates, national ID numbers and addresses. The defendant alleged that this was done to inform the local community of the circumstances of the case because residents had expressed great concern. The Taichung District Court found that in the absence of consent from the plaintiff, the defendant's actions constituted infringement of the plaintiff's privacy. The Taichung Court ruled that even though there was no malicious intent, the civil law principle that one must be held liable for his actions applied and the defendant was ordered to pay 5,000 NTD (approx. USD 170) to each of the plaintiffs for mental suffering. The relatively small awards of damages can be contrasted with the damages claimed by the plaintiffs: 140,000 NTD (approx. USD 4,766) and 120,000 NTD (approx. USD 4,080).

Criminal cases

(102) Shenjian Zi No. 1059 (Taipei District Court, 2013): In a case decided by a Taipei Court, an individual was convicted after disclosing private information through faxes. After a water leak continued in spite of repairs to the water tank, the accused faxed messages attacking the reputation of the complainant and disclosed the complainant's personal information. The Taipei Court applied PIPA 41(1) and Article 310(2) of the Criminal Code (libel). The defendant was found guilty of slander and using personal information outside the scope of the purpose of collection. Since the convictions were for different conduct, the Court decided not to merge the sentences. The individual was condemned to two months of detention convertible to a fine.

(102) Yi Zi No. 317 (Taichung District Court): In a case decided before a Taichung Court, the complainant and a married couple had a dispute arising out of interference in family relations, adultery, and an abortion. The defendant (the wife) posted disparaging messages under an alias on Facebook and Wretch (a defunct blogging platform) disclosing the alleged adultery and abortion. The messages also disclosed the personal information of the complainant.

The Court found that Facebook and Wretch website were public Internet platforms. By publishing these statements, the defendant harmed the reputations of the complainant under circumstances that constituted aggravated slander under Article 310(2) of the Criminal Code. According to the Court, the defendant also divulged personal information in contravention of Articles 19 and 41 of PIPA (protection of personal data and divulgation of private information respectively). In the end, the Court did not enter a final judgment because the defendant and the complainant reached an out-of-court settlement.

Implications of the PIPA in practice

Use by private individuals: This review of the still relatively small number of cases decided under PIPA suggests that fears that the courts

 © 2014 PRIVACY LAWS & BUSINESS

would actively enforce the PIPA against corporations and impose huge judgments have been overstated. Indeed, there have been few if any PIPA cases against corporate defendants. What these cases show is that those affected by the PIPA have thus far been average citizens embroiled in disputes with their neighbors or who use social media such as Facebook and blogs to attack people and to disseminate private information.

The decided cases tend to arise in the context of the private lives of ordinary citizens. There is a recurring pattern in which individuals are sanctioned for imprudently disclosing personal information about others in the course of petty disputes resulting relatively harsh penalties and heavy liability by Taiwanese standards. This use of the PIPA may not have been anticipated by policy makers in the executive branch who drafted the law nor considered by the legislators who enacted it. One of the amendments to the Act now before the Legislature proposes to decriminalize the disclosure of personal information if the disclosure is not for profit. Until then, there is a real threat of criminal penalties being imposed especially for disclosures made through social media.

Corporate liability and class actions: None of the victims whose private information was disclosed by Far Eastern International Bank or Nokia Taiwan have brought lawsuits against the companies. This may be because these firms have already dealt with the issue and settled with the victims, or because these potential plaintiffs were deterred by the high technical demands or economics of such claims.

Under the PIPA, a group of at least 20 similarly situated plaintiffs can at least theoretically bring a class action privacy claim through a qualified non-profit association class action. However, no qualified association has been incorporated for this purpose, nor have preparatory steps been taken to do so.[1] Once a qualified association has been established, it must operate for at least three years before it has standing to bring a class action on behalf of a group of plaintiffs. Therefore, even if there were a group of individuals willing to bring class action today, it does not appear that they would be able to do so for at least another three years because no association exists with clear standing. In the meantime, corporations that collect and use large amounts of personal information should use this breathing space as an opportunity to improve compliance with the PIPA and educate their employees about the law.

Freedom of information: A step backwards? One of the recurring criticisms of the PIPA is that it has become, in practice, a convenient excuse for the executive branch to refuse to provide citizens with previously public information on grounds that it is personal information. For example, the Judicial Yuan has issued regulations prohibiting recording the statements of any person who appears in court without their written permission.[2] Another example was the Control Yuan's decision to remove historical financial information reported by politicians under Taiwan's sunshine laws from its website.[3]

Most Taiwanese are aware that one of the reasons PIPA was passed was to thwart the collection of personal data by those groups which specialize in defrauding citizens. This is why the duties imposed on 'non-governmental agencies' are so stringent. At the same time it appears that not enough thought has been given to the question of how governmental bodies should protect personal information. 'Non-governmental bodies' (i.e. the private sector) are supervised by public agencies responsible for various sectors, but nobody is responsible for supervising these governmental agencies. The result has been certain overzealousness in protecting personal information from the public that has allowed a historically reticent government to backtrack on recent moves toward greater transparency.

Administrative developments: Another concern with the PIPA and its enforcement is that it did not create a single data protection authority. Under the PIPA, regulatory authority is dispersed between a number of agencies at different levels of government: (i) the general central government authority and (ii) the central and local authorities supervising specific industries. The Ministry of Justice acts as an unofficial general central government authority while individual agencies regulate their specific remits. For example, the Financial Supervision Commission regulates data protection in the financial industry.

Before the PIPA was enacted, the Ministry of Justice (the "MOJ") played a coordinating role in bringing the PIPA into force and took responsibility for drafting the PIPA's Enforcement Rules. Whether it will continue to be responsible for coordinating the enforcement of PIPA or for providing statistical information about administrative enforcement remains to be seen. While the private sector is supervised by public agencies responsible for various sectors, the MOJ is not responsible for supervising how governmental agencies comply with the PIPA.

During the first year the PIPA was in effect, the MOJ played a limited role in actual enforcement. Nevertheless by the end of 2013, the MOJ published a number of guidance documents including forms for relevant authorities to report activities related to PIPA to MOJ[4], an online 'handbook' compiling all the existing sources of law in relation with PIPA, and a report listing all of its databases containing personal information. These measures may have been

REFERENCES

1 We understand that the Consumers' Foundation is studying whether it may have standing to bring data protection class actions. This is Taiwan's oldest consumer protection group and has standing to bring product liability class actions. They have received inquiries but do not believe that data protection is part of their core mission. An association's standing to bring a privacy class action under the PIPA would be vigorously challenged if it were not founded for the primary purpose of furthering data protection interests.

2 Regulations Governing Court Room Recording, Use, and Preservation. Issued 25 October 2013.

3 See *Liberty Times* "Using Personal Information Protection as an excuse: Control Yuan removes reported financial information from before July 2010" 2013-9-1; last accessed 2014-2-2. Financial information from before July 2010 remains publicly accessible at the Control Yuan by consulting hard copies of the Control Yuan's gazetteer.

4 www.moj.gov.tw/public/Attachment/37811193966.xlsx

intended to encourage other authorities to follow the MOJ's lead.

Other industry-specific authorities have also issued over 40 guidelines on how the PIPA shall be enforced in their particular domain.

Conclusion

One year after the PIPA became operative, the Courts are hearing a growing number of PIPA cases brought by individuals under the PIPA while impact on the corporate sector has been less than expected. Government agencies have implemented measure to protect that the vast amounts of personal information they hold with a somewhat negative effect of freedom of information. Undoubtedly, the most significant effect of the PIPA has been to create widespread awareness of data protection and privacy issues on all levels of society even if administrative enforcement and legal remedies have not yet been fully developed.

AUTHOR

Chen Hui-ling is a Partner at law firm Winkler Partners in Taipei, Taiwan
Email: hchen@winklerpartners.com

EU LIBE pushes for action on NSA surveillance and recommends suspension of US Safe Harbor

The European Parliament's LIBE Committee's (Committee on Civil Liberties, Justice and Home Affairs) draft report on the 'US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs' says that the Parliament should vote on the following measures to ensure follow up action in the next Parliament:

1. **Adopt the Data Protection Package** in 2014.
2. **Conclude the EU-US Umbrella agreement** ensuring proper redress mechanisms for EU citizens in case of data transfers from the EU to the US for law enforcement purposes.
3. **Suspend Safe Harbor** until a full review is conducted and current loopholes are remedied making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with EU highest standards.
4. **Suspend the TFTP** [Terrorist Finance Tracking Programme] agreement until i) the Umbrella agreement negotiations have been concluded; ii) a thorough investigation has been concluded based on EU analysis and all concerns raised by the Parliament in its resolution of 23 October have been properly addressed.
5. **Protect the rule of law and the fundamental rights** of EU citizens, with a particular focus on threats to the freedom of the press and professional confidentiality (including lawyer-client relations) as well as enhanced protection for whistleblowers.
5. **Develop a European strategy for IT independence** (at national and EU level).
6. **Develop the EU as a reference player** for a democratic and neutral governance of the Internet.

- *See http://tinyurl.com/lntpyva*

US defends Safe Harbor citing economic benefits as 12 firms settle FTC charges

The US Department of Commerce's International Trade Administration published a 'Key Points' document in January 2014 which provides additional information about the enforcement of the EU-US and US-Swiss Safe Harbor frameworks.

The document discusses the benefits of the programme stating that it brings economic benefits. The Department of Commerce says that: "Many US organizations that self-certify to Safe Harbor do so at the express request of European customers/clients or partners, while others are actually US subsidiaries or divisions of European organizations."

"Claims of Safe Harbor participation can easily be verified by searching the official Safe Harbor List(s) to determine whether a given organization is on the List(s), and if it is, whether its Certification Status is current or has lapsed."

At the same time, the Federal Trade Commission (FTC) announced that 12 US businesses had agreed to settle FTC charges that they falsely claimed they were abiding by EU-US Safe Harbor. Under the proposed settlement agreements, "the companies are prohibited from misrepresenting the extent to which they participate in any privacy or data security program sponsored by the government or any other self-regulatory or standard-setting organization".

These activities have been prompted by the EU Commission's demands that the US improves the functioning of the scheme by summer 2014 [*PL&B International* December 2013, p. 6] and were initiated by complaints by Chris Connolly, Director, Galexia, [*PL&B International December 2008* p.1] he explained to *PL&B* last month in Brussels.

- *See the Key Points document at http://export.gov/static/Safe%20Harbor%20Key%20Points%2012-2013_Latest_eg_main_068867.pdf*
The list of companies that settled with the FTC is at: www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply

 © 2014 PRIVACY LAWS & BUSINESS