

University of New South Wales
University of New South Wales Faculty of Law Research Series
2012

Year 2012

Paper 26

Data Privacy Enforcement in Taiwan, Macau,
and China

Graham Greenleaf*

Hui-ling Chen†

*University of New South Wales

†Winkler Partners

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps12/26>

Copyright ©2012 by the authors.

Data Privacy Enforcement in Taiwan, Macau, and China

Graham Greenleaf and Hui-ling Chen

Abstract

This article, the third in a series surveying significant recent examples of data privacy enforcement actions in Asia-Pacific jurisdictions, covers the Chinese-speaking Asian jurisdictions, other than Hong Kong: Taiwan and Macau SAR with general data privacy laws, plus the Peoples Republic of China where there has been significant enforcement under a variety of law laws.

In Taiwan the *Computer Processed Personal Data Protection Act* (CPPDPA) is still in force, as the new *Personal Information Protection Act* (PIPA) has not yet been brought into force. There were no significant examples of administrative enforcement actions by the responsible Ministries in 2011 under the current CPDPA. Nor have there been any in the nearly 20 years that the Act has been in force. Enforcement of the Act has been haphazard and intermittent at best. The main reason has been that no single agency has the responsibility of enforcing the Act. In contrast, the new *Personal Information Protection Act* (PIPA) identifies the Ministry of Justice (MOJ) as the agency responsible for coordinating enforcement of the new Act. Despite the lack of Ministerial enforcement, there has been some enforcement via the Courts. Over the past 10 years, Taiwan's high courts have decided about 30-40 civil claims for damages under the current Act. Only three were successful. The current Act also has criminal penalties, and during that 10 year period about 100 criminal cases under the Act have reached the high courts with convictions resulting in about sixty per cent of cases. Separate from the data protection law, there were important administrative enforcement action by Taiwan's financial services super-regulator, the Financial Supervisory Commission (the FSC) in 2009 and 2010 against banks on privacy-related grounds. The article includes examples of the various successful enforcement actions.

Macau's Office for Personal Data Protection (OPDP) has administered *Personal Data Protection Act* since 2007, and has very extensive powers. The article details the enforcement actions it took in 2011 and early 2012, notable for their greater use of concepts derived from European data protection law than other European jurisdictions, in relation to matters such as Google's Streetview, government recording of complaint calls, disclosure of information about shoplifters and debtors, direct marketing, and mobile surveillance by the Security Police.

Although the Peoples Republic of China does not have a comprehensive data protection law, examples of privacy enforcement in China occur increasingly. Recent examples of Court decisions and prosecutions are under a diverse range of laws and rulings that result in privacy enforcement. The article gives examples of criminal prosecutions and a significant court ruling confirming the right of citizens to take action against government agencies for wrongful publication of personal information.

In all of the Chinese-speaking jurisdictions, privacy laws are being enforced, but in different ways. In Hong Kong (examined in the previous article), there is an enforcement but it is of limited effectiveness. In Macau, fines of modest size seem to be the norm for any breach of the legislation. In Taiwan, administrative enforcement by the financial regulator is resulting in substantial financial penalties for privacy breaches on a regular basis, based on the financial regulation law. In the Peoples Republic a wide variety of criminal enforcement measures are being used, with penalties often including jail terms, but complaints or civil actions by individuals are less prominent as yet.

Data privacy enforcement in Taiwan, Macau, and China

Graham Greenleaf and Chen Hui-ling*

Graham Greenleaf is Professor of Law & Information Technology, University of New South Wales; Chen Hui-ling is a Partner at Winkler Partners, Taipei, Taiwan

Privacy Laws & Business International Report, Issue 117, 11-13, June 2012

14 May 2012

Contents

Taiwan	1
Little enforcement under the data protection law.....	2
Enforcement via the Courts	2
Strong privacy enforcement by a financial regulator	2
Macau SAR	3
Peoples Republic of China (PRC)	4
Criminal prosecutions	4
Civil actions	5
Conclusions	5

This article is the third in a series¹ surveying significant recent examples of data privacy enforcement actions in Asia-Pacific jurisdictions², most occurring since 2011. This article covers the Chinese-speaking Asian jurisdictions, other than Hong Kong: Taiwan and Macau SAR with general data privacy laws, plus the Peoples Republic of China where there has been significant enforcement under a variety of law laws. The final article will consider South Korea, Japan, Indonesia and other Asian countries.

Taiwan

In Taiwan the *Computer Processed Personal Data Protection Act* (CPPDPA) is still in force, as the new *Personal Information Protection Act* (PIPA) has not yet been brought into force.

* Graham Greenleaf is Professor of Law & Information Technology, University of New South Wales; Chen Hui-ling is a Partner at Winkler Partners, Taipei. Thanks for assistance to Ken Yang of the Macau Office for Personal Data Protection, and Paul McKenzie and Jingxiao Fang of Morrison & Foerster, Beijing Office

¹ See Greenleaf G and Evans K 'Privacy enforcement strengthens in Australia & New Zealand' (2012) 115 PLBIR 8-13; and Greenleaf G and McLeish R 'Hong Kong's privacy enforcement: Issues exposed, but powers lacking' (2012) 115 PLBIR 2528

² By 'significant examples of privacy enforcement actions' what we mean is as follows. First, the action results from complaints to an authority/Court, or 'own motion' actions by an authority responding to a specific situation. (General investigations or reform proposals by authorities are not included). Secondly, the authorities concerned could be Data Protection Authorities/Privacy Commissioners but they could also be telecommunications regulators, financial regulators, government agencies and so on. Independent industry self-regulatory bodies could also be included. Court or Tribunal decisions of any type are also included. Third, the result is a significant remedy for an individual; or a remedy for a group of people; or a significant change in the interpretation of the law; or a significant change in business/government practices.

Little enforcement under the data protection law

There were no significant examples of administrative enforcement actions by the responsible Ministries in 2011 under the current CPPDPA. Nor have there been any in the nearly 20 years that the Act has been in force. Enforcement of the Act has been haphazard and intermittent at best. The main reason has been that no single agency has the responsibility of enforcing the Act. Instead, it fragments the authority to sanction between the various government agencies who supervise the limited number of industries or sectors to which the current Act applies. The Ministry of Communications is responsible for sanctioning telecommunications enterprises that violate the current data protection act, the Department of Health is responsible for hospitals, the FSC is responsible for financial services, and so on. None of these agencies sees the policing of compliance with data protection laws as a core role. Most agencies seem unaware of their duties under the Act and have no centralized means of tracking enforcement actions, making it difficult for reliable enforcement information to be obtained.

In contrast, the new *Personal Information Protection Act* (PIPA) identifies the Ministry of Justice (MOJ) as the agency responsible for coordinating enforcement of the new Act (see PLBIR Issue 114, December 2011, 24-26), and it appears to be taking its new duties seriously. It is likely that administrative enforcement under the new Act will become more systematic and that the Ministry will provide statistics regularly, as Taiwanese government agencies do for their core competencies. It is the sole competent authority for drafting the Enforcement Rules (A 55). The MOJ works with other government agencies in charge of a particular industry at the central government level. The specific purpose and the classification of personal information stipulated in the PIPA should be prescribed by the MOJ in conjunction with the government authority in charge of a particular industry (A 53).

Enforcement via the Courts

Despite the lack of Ministerial enforcement, there has been some enforcement via the Courts. Over the past 10 years, Taiwan's high courts have decided about 30-40 civil claims for damages under the current Act. Only three were successful. The largest award of damages was NT\$80,000 (c. US\$2,700), with awards of NT\$20,000 to NT\$50,000 in the other two cases. In the first case, an insurance company's employee sent one customer A's personal information to customer B. In the other two cases, the company failed to implement measures to protect data or implemented inadequate measures, this caused it to disclose customer data wrongfully (i.e. without consent). In the third case, the bank's failure to adequately protect customer data allowed a third party to find the customer data with an Internet search.

The current Act also has criminal penalties, and during that 10 year period about 100 criminal cases under the Act have reached the high courts with convictions resulting in about sixty per cent of cases. In many of the cases, the violation of the CPPDPA is a lesser included offence and the sentence imposed is for the greater offence under other legislation (criminal breach of trust, fraud etc), so there is little indication of what sentences would result for breaches for the CPPDPA alone. The most common violation was for failure to apply for a license and thereby unlawfully collecting and selling personal data for profit (A 19 of CPPDA).

Strong privacy enforcement by a financial regulator

Separate from the data protection law, there were important administrative enforcement action by Taiwan's financial services super-regulator, the Financial Supervisory Commission (the FSC) in 2009 and 2010 against banks on privacy-related grounds. The FSC has also imposed privacy-related sanctions on two insurance brokers and one life insurance company in March 2012. The FSC is modeled in part on the UK's Financial Services Authority, and is a very aggressive and pro-active regulator. Rather than waiting for the PIPA to come into effect, the FSC has been imposing very substantial fines (by Taiwan's frugal standards) on banks and insurance brokers for privacy-related

transgressions. It has not based its penalties on the authority of the CPPDPA, but has relied on its regulations requiring internal controls at financial institutions. The FSC has very wide statutory authority to mandate internal controls.

In both 2009 and 2010, the FSC fined two different banks NT\$4,000,000 (US\$130,000) for failing to implement required data security measures resulting in disclosures of personal information about bank customers. According to media reports, the 2010 case involved a hacker attack on E.Sun Bank in which a hacker was able to insert a trojan computer program to exploit a security weakness. Although no losses were reported by the bank's auditors, the hacker was able to obtain personal information regarding some 10,000 account holders. There are very few details available about the breach of security systems at Taishin Bank in 2009, but it appears to be related to disclosure of credit card transactions and card-holder personal information. Neither Taishin nor E.Sun appear to have exercised their right to file administrative and legal appeals against these fines. In contrast, the FSC normally fines banks from NT\$20,000 to NT\$100,000 (US\$666 - US\$3,300) for violations of the CPPDPA, in its role as the government authority for that sector.

In March 2012 the FSC fined two insurance brokers NT\$600,000 (US\$20,000) each because the brokers had illegally released personal information about policy holders to a life insurance company to help the life insurer market its policies. Again, these fines were not based on Taiwan's data protection laws *per se*, but were based on the rules for internal controls at financial institutions. The life insurance company was also fined NT\$100,000 (US\$3,300). However, this fine was imposed for violating the current data protection act and the FSC's requirements for internal controls in insurance businesses. One reason the FSC may prefer to use its rules for internal controls to sanction data protection breaches is that the maximum fines are much higher than those available under the CPPDPA.

Macau SAR

The Office for Personal Data Protection (OPDP) has administered Macau's *Personal Data Protection Act* (PDPA) since 2007, and has very extensive powers³. It took the following enforcement actions in 2011 and early 2012, notable for their greater use of concepts derived from European data protection law than other European jurisdictions:

- Google was fined MOP30,000 (US\$3,750) for breaching the PDPA because its Street View mapping service in 2008, when it collected images in the streets of Macao that are narrow with many alleys crisscrossing each other, was considered to be the collection of sensitive data that may reveal one's private life, etc. without necessary authorization from OPDP. Google also breached the privacy law by illegally collecting WiFi and payload data from open WiFi networks and transferring personal information obtained from Macao's WiFi data to US. Google has paid the fine for the three offenses.
- A government agency was fined for MOP8,000 (US\$1,000) for recording telephone complaint calls without proper consent. It had set up the telephone recording system to assist handling telephone complaints, and to evaluate staff performance. The system failed technically to provide the automatic voice reminder function to inform callers that their conversations will be recorded. The agency's staff then failed to give a verbal notification before recording a complainant's call, and without obtaining his consent. This revealed a systematic failure to obtain proper consents from the data subject, and the agency was held to therefor lack the legitimacy for processing the complainants' data.

³ See Greenleaf, G "Macao's EU-influenced Personal Data Protection Act" (2008) 96 *Privacy Laws & Business International Newsletter*, available at <<http://www.austlii.edu.au/au/journals/ALRS/2008/9.html>>

- A retail business was fined MOP10,000 (US\$1,250) for again publicising photos and videos of suspects alleged to have stolen items from their shops. It had installed surveillance systems to safeguard its property or other legitimate interests. However the publication was held to be a violation of the principle of proportionality.
- A telephone company was fined MOP4,000 (US\$500) for mistakenly sending a customer's bills to another unrelated persons' e-mail address over a 10-month period, for failing to take adequate measures to keep its customers' data in its database accurate and up to date, as well as not taking appropriate security measures to protect its customers personal data.
- A self-employed decorating contractor was fined MOP4,000 (US\$500) for disclosure his debtor and the debtor's wife's personal information. He held a press conference and disclosed the debtor's residential address in full. This was held to be a violation of the principle of proportionality. However, in relation to the debtor's complaint against two newspapers because they reported his residential address in full, OPDP held that freedom of press was protected by the Publication Law, and he could only lodge his complaint to a court by civil litigation.
- A local Bank was fined for MOP4,000 (US\$500) for sending its former client a SMS for direct marketing, neglecting the client's request to stop doing so made under his Right of Objection.

In another significant decision, ODPD intervened to cause the suspension of the use of mobile traffic surveillance cameras by the Traffic Services Bureau and the Public Security Police because it lacked legitimacy, in that the use might involve the collection and processing of sensitive data outside the sphere of public roads.

Peoples Republic of China (PRC)

Although China does not have a comprehensive data protection law, it would be incorrect to think that examples of privacy enforcement in China are rare or non-existent. The following recent examples of Court decisions and prosecutions illustrate the diverse range of laws and rulings that result in privacy enforcement. The seriousness with which misuse of personal data is seen by Chinese authorities is reflected in an editorial in the *China Daily*⁴:

A recent survey found that in the last six months of 2011 alone, 121 million Internet users had their account numbers and their secret codes stolen. It is not being alarmist to forecast that the booming trade in personal information and its illegal use will finally ruin online economic activities and disturb even the order of off-line business activities. A law is obviously needed to deter the unauthorized use of personal information.

Criminal prosecutions

- The People's Court in the Longgang District of Shenzhen Municipality held that a defendant who had obtained photocopies of the identity cards of 2,000 people either through illegal purchase or exchange on the Internet, and then sold the information, was guilty of the crime of unlawfully accessing personal information of third parties and sentenced to a one-year prison term and a fine of RMB1,000, applying provisions of the PRC Criminal Law. This was the first personal information breach case in Longgang District, and occurred in

⁴ Editorial 'Personal data protection' *China Daily* 6 April 2012 at <http://www.chinadaily.com.cn/opinion/2012-04/06/content_14987674.htm>

October 2011, shortly before amendments tightening the Identity Card Law were promulgated (as summarised by McKenzie and Fang⁵).

- China's State Council Information Office (SCIO), announced in January 2012 the arrest of four persons and punishment of eight others for attempts to resell data or fabricate rumors about online data leaks in relation to China Software Development Network (CSDN, a discussion forum for software developers) and online forum Tianya. CSDN admitted that the information of around 6 million users had been posted online⁶.
- The Beijing Second Intermediate People's Court issued a judgment in one of the biggest personal information breach cases to date in Beijing in August 2011. Twenty three defendants, employees of a telecommunications company, illegally sold personal information such as personal phone numbers of the company's subscribers. The court held that the sale infringed the legitimate rights and interests of the subscribers and caused serious damages, and imposed jail terms ranging from 6 to 30 months⁷.
- Although not yet at the stage of prosecutions, it is reported that Dun & Bradstreet has suspended operations at one of its Shanghai businesses pending inquiries by both Chinese and US authorities. The reports said the D&B company had income level, jobs and addresses details and other personal information, for 150 million Chinese residents and that individuals' details had been sold for 23¢ each to companies involved in telemarketing. The report said the company's data sources included banks, insurance companies, real estate agents and telemarketers⁸.

Civil actions

The Supreme People's Court has issued Provisions stipulating that a citizen, legal person or organization can file an administrative lawsuit against the government if it considers that government publication of information infringes upon its individual privacy or trade secrets⁹. Where breaches are proven, the court may order that the disclosure is illegal and order the government to take remedial measures (*Provisions on Several Issues regarding the Hearing of Administrative Cases Involving Public Government Information*, in force August 13, 2011). This court ruling is very significant, confirming the right of citizens to take action against government agencies for wrongful publication of personal information. The *Tort Liability Law* of 2009 also provides a specific right in citizens to sue other private parties for damages and other remedies for infringements of privacy. As yet, civil cases under either of these provisions are not reported.

Conclusions

In all of these Chinese-speaking jurisdictions, privacy laws are being enforced, but in different ways. In Hong Kong (examined in the previous article in this series), there is an enforcement but it is of limited effectiveness, due to the Commissioner having no powers to take issue any penalties provided that breaches stop occurring, and the Court issuing fines that are too low to act as a

⁵ McKenzie P and Fang J 'China's Online Data Privacy Rules Coming into Effect; Other Recent Data Privacy Developments in China' *Morrison & Foerster Client Alert*, 23 February 2012

⁶ Special Correspondent 'Four Tied To Data Breaches Arrested; Web Hack Investigation Results Set Out' (2012) 12 WDPR 32 *Bloomberg BNA World Data Protection Report*, 30 January, 2012

⁷ As summarised by McKenzie and Fang, cited above

⁸ Joyanta Acharjee 'Dun & Bradstreet suspends China unit operations in data privacy probe' Proactive Investors website, 19 March 2012 at <<http://www.proactiveinvestors.com/companies/news/26464/dun-bradstreet-suspends-china-unit-operations-in-data-privacy-probe-26464.html>>

⁹ From a summary by McKenzie and Fang, cited above

deterrent against continuing breaches. In Macau, fines of modest size (US\$500 - \$3750) seem to be the norm for any breach of the legislation. This is hardly substantial, but it is more than in Hong Kong. In Taiwan, administrative enforcement by the financial regulator is resulting in substantial financial penalties (two cases of US\$130,000 and one more recent case of US\$20,000) for privacy breaches on a regular basis, based on the financial regulation law and not on the existing data protection law. In other sectors there is little administrative enforcement of the data protection law although there is some enforcement by civil and criminal actions in the Courts. In the Peoples Republic a wide variety of criminal enforcement measures are being used, with penalties often including jail terms, but complaints or civil actions by individuals are less prominent as yet.

