COMPUTER LAW & SECURITY REVIEW 32 (2016) 375–380

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia-Pacific news

Gabriela Kennedy *

Mayer Brown JSM, Hong Kong

Keywords:
Asia-Pacific
IT/information technology
Communications
Internet
Media
Law

ABSTRACT

This column provides a country by country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

Gabriela Kennedy *(Partner), Mayer Brown JSM (gabriela.kennedy@mayerbrownjsm.com);* **Karen H.F. Lee** *(Senior Associate), Mayer Brown JSM (karen.hf.lee@mayerbrownjsm.com).*

1.1. *How much is that data in the window? Individual convicted for transferring personal data to third party for direct marketing purposes*

On 30 December 2015, an individual was convicted for breaching the direct marketing provisions under the Hong Kong Personal Data (Privacy) Ordinance ("**PDPO**"). This conviction closely follows 3 earlier convictions in September and November 2015, respectively, and marks the first conviction against an individual for the transfer of personal data to a third party for use in direct marketing, without obtaining valid consent.

1.1.1. *Relevant PDPO provisions*

The new direct marketing provisions introduced by the Personal Data (Privacy (Amendment) Ordinance 2012 came into effect on 1st April 2013. Under the new Sections 35C and 35J of the PDPO, data users are prohibited from using an individual's personal data for direct marketing purposes, or from transferring an individual's personal data to a third party for their use in direct marketing, unless the individual has provided his/her express prior consent.

To obtain valid consent for the transfer of personal data to a third party, for them to use such personal data to market their own products and services, the data user must have notified the individuals of the following:

(a) that it intends to transfer their personal data for direct marketing purposes, and cannot do so without their consent;
(b) the classes of transferees to whom their personal data will be transferred;
(c) the type of personal data that will be transferred;
(d) the classes of goods, facilities or services that will be marketed by the third party recipient;
(e) whether the personal data are being transferred in return for gain (e.g. in return for payment, etc); and
(f) a response channel through which the individual can communicate his/her consent in writing (without charge).

The consent for such transfer must be obtained in writing. Breach of the direct marketing provisions is a criminal offence and may result in a maximum fine of HK$ 500,000 or HK$1,000,000 and up to 3 or 5 years imprisonment (depending on the gravity of the breach).

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong. Tel.: +852 2843 2211.
E-mail address: gabriela.kennedy@mayerbrownjsm.com.

http://dx.doi.org/10.1016/j.clsr.2016.01.002
0267-3649/

1.1.2. *The case*

In April 2014, the Hong Kong Office of the Privacy Commissioner of Personal Data ("**PCPD**") received a complaint against a real estate agent and an insurance agent. The complainant alleged that the real estate agent had obtained the data subject's name and mobile phone number (the "**Personal Data**") at a social function. The real estate agent subsequently provided the Personal Data to an insurance agent for her use in direct marketing. The real estate agent did not notify or seek the complainant's prior consent before transferring his Personal Data. The insurance agent called the complainant two months later, identified herself as a financial planner of an insurance company and informed the complainant that the first defendant had given her the Personal Data. The complainant refused to engage further with her when he realised the insurance agent intended to market to him financial planning and insurance products.

The case was referred by the PCPD for prosecution and brought before the Eastern Magistrates' Court. The real estate agent was found to have committed an offence under Section 35J of the PDPO as a result of him transferring the Personal Data to the insurance agent without the complainant's consent and was ordered to pay a fine of HK$5000. The insurance agent was charged with the offence of using personal data in direct marketing without taking specified actions under Section 35C of the PDPO but was acquitted as the magistrate could not dismiss the possibility of her attempting to take such actions had the complainant not hung up on her, the first time she contacted him.

1.1.3. *Courts continuing with hard-line approach?*

This latest case is just one of a series of convictions in the last half of 2015, for breach of the direct marketing provisions[1] under PDPO. On 9 September 2015, a telecommunications company was convicted for failing to comply with an individual's request to cease receiving direct marketing materials and was fined HK$ 30,000. This case was closely followed by another conviction against a relocation and storage company on 15 September 2015, for its failure to comply with the notification requirements and to obtain consent for the use of the complainant's personal data in direct marketing. The storage and relocation company was fined HK$ 10,000. On 3 November 2015, a company that provides body check services was also convicted for failing to comply with a client's request to no longer receive direct marketing materials and was subject to a fine of HK$ 10,000.

The actual fines imposed by the Hong Kong courts so far are relatively small. While such fines may be commensurate with the breach, prison sentences and higher fines should not be ruled out for more egregious cases, such as where a large volume of personal data has been sold or transferred to a third party for direct marketing purposes, without obtaining the required consent.

Irrespective of the level of fine imposed, the damage to the reputation of a data user in the event of a conviction can be a much harsher punishment and one from which it may take a long time to recover.

1.1.4. *Takeaway points*

The recent case highlights the fact that the courts are not only willing to convict companies, but are also willing to hold individuals accountable for breaches of the PDPO. Collection of data in a social context does not imply consent and certainly cannot imply consent for the transfer of data to third parties.

2. China

Gabriela Kennedy *(Partner), Mayer Brown JSM (*gabriela.kennedy@mayerbrownjsm.com*);* **Xiaoyan Zhang** *(Of Counsel), Mayer Brown JSM (*xiaoyan.zhang@mayerbrownjsm.com*).*

2.1. *China passes counter-terrorism law*

On 27 December 2015, the National People's Congress Standing Committee passed China's new Counter-Terrorism Law (New Law), which came into effect on 1 January 2016. Compared to the Draft Counter-Terrorism Law ("**Draft Law**") that was first released on 3 November 2014 for public reading, the New Law appears less draconian as two, much objected, key requirements have been dropped. These requirements were: (i) telecommunication service operators and Internet service providers (together, "**ISPs**") must "locate their related servers and domestic user data" in China (the "**Localisation Requirement**"), and (ii) must install "technical interfaces in the design, construction, and operation of the telecommunication and internet [services]" that would allow Chinese government to "prevent" or "investigate" terrorist activities (the "**Backdoor Requirement**"). The New Law, however, retains two key requirements from the Draft Law, i.e., that ISPs shall disclose encryption keys to government authorities (the "**Decryption Requirement**") and shall enhance monitoring and reporting of all Internet content (the "**Reporting Requirement**"). The respective exclusions and inclusions bring some relief to the international tech community but trigger concerns for others.

Specifically, Article 18 of the New Law requires that ISPs "shall provide technical interfaces, decryption and other technical support and assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with the law." This Decryption Requirement overlooks the fact that an increased number of communications products nowadays use "end-to-end" encryption where the software vendors themselves do not retain any decryption keys. The only way to meet the Decryption Requirement in such cases is to surrender users' passwords, putting the issue of privacy at risk. So far, the United States, home to many tech companies, has expressed the greatest resistance to the New Law as the Decryption Requirement appears to target vendors whose products, including smartphones and tablets, feature end-to-end encryption.

The Reporting Requirement is illustrated in Article 19 of the New Law, requiring ISPs to "put into practice network

[1] Please refer to our Legal Update "Two Companies Convicted for Breach of the Direct Marketing Provisions under the Hong Kong Personal Data (Privacy) Ordinance" published on 16 September 2015: https://www.mayerbrown.com/files/Publication/e1349067-d2c0-4cf8-b45c-2dcf10fabf9c/Presentation/PublicationAttachment/aebd35df-c0d6-42e7-8f37-373c58e083ff/150916-HKG-PrivacySecurity-Litigation-TMT.pdf.