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. *The pitfalls of networking: individual's conviction upheld for transferring personal data for direct marketing purposes*

On 2 June 2017, the Court of First Instance (**"CFI"**) upheld the conviction of the Eastern Magistrates' Court against an individual, for breach of the direct marketing provisions under the Personal Data (Privacy) Ordinance (Cap. 486) (**"PDPO"**).

1.1.1. *Restrictions on transfer*

Under the PDPO, a data user cannot transfer an individual's personal data to a third party for their use in direct marketing, unless the prior written consent of the individual has been obtained. Any such consent will only be valid if the data user has notified the individual of the following:

(a) that it intends to transfer the individual's personal data to a third party for direct marketing purposes, and cannot do so without their consent;
(b) the classes of recipients 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 is being transferred in return for gain (e.g. in return for payment, etc); and
(f) a response channel through which the individual can communicate their consent in writing (without charge).

Breach of the direct marketing restrictions amounts to a criminal offence and can incur a hefty fine, the maximum of which is HK$1,000,000 and up to 5 years imprisonment (depending on the gravity and nature of the breach).

1.1.2. *The case*

During a social function, the defendant had collected the name and phone number of an individual (**"Complainant"**). The defendant subsequently transferred the Complainant's personal data to an insurance agent, without notifying or obtaining the Complainant's consent prior to the transfer of the personal data.

For further information see: www.mayerbrown.com.

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

http://dx.doi.org/10.1016/j.clsr.2017.07.002
0267-3649/

Please cite this article in press as: Gabriela Kennedy, Asia Pacific news, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.07.002

The insurance agent called the Complainant, identifying herself as a financial planner of an insurance company, and informed the Complainant that the defendant had provided her with the Complainant's name and phone number. The Complainant ended the call when he realized that the insurance agent was calling for the purposes of promoting financial planning and insurance products.

In April 2014, the Complainant issued a complaint to the Hong Kong Office of the Privacy Commissioner of Personal Data ("**PCPD**"). The PCPD subsequently referred the matter for prosecution and the case was brought before the Eastern Magistrates' Court. The defendant 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$5,000.

The defendant appealed the Magistrate's decision. The CFI upheld the lower court's finding that the defendant's act of sharing the Complainant's personal data with the insurance agent, without obtaining his prior consent, knowing that the insurance agent may use the data to try and sell insurance products, amounted to a breach of the PDPO. Whether the insurance agent had actually ended up using the personal data for direct marketing purposes was irrelevant. The CFI also confirmed that the word "offer" in the context of the definition of direct marketing under the PDPO, should be interpreted broadly to include mere acts of suggesting or alluding to the possibility of providing a product or a service. This would therefore capture direct-marketing communications that ended at an early stage, due to the data subject expressing his lack of interest at the outset in the product or service being marketed.

A number of decisions issued at Magistrate Court level have gone on appeal to the CFI. So far, the High Court has upheld the decisions of the lower courts in relation to direct marketing convictions under the PDPO. On 27 January 2017, the High Court upheld the Tsuen Wan Magistrates' Court's landmark conviction of 2015 in which the internet service provider, Hong Kong Broadband Network Limited, was fined HK$30,000 for breach of the direct marketing provisions[1].

1.1.3. *Individuals as data users*

The recent decision draws attention to the fact that individuals as data users are subject to the PDPO if they collect and use personal data, just like a data user that is a corporate body. Given the ubiquitous collection of data through apps, it appears that the spotlight is now shifting to individuals as data users. The PCPD has raised recent concerns in relation to individual app users who have allowed apps to collect personal data stored in their phone books on their mobile device.

In May 2017, it was found that an app known as DU Caller, had been collecting and using personal information without the knowledge or consent of relevant data subjects. Whilst DU Caller allows users to filter and block unwanted or suspicious calls, it also provides a "reverse look-up" function for users to input a number to identify the holder of that phone number, and to search for phone numbers using the name of an organization or individual. The database of phone numbers and names was compiled from the phone books of the app users, which were allegedly collected by the operator of DU Caller without the consent of the holders of the phone numbers, or sometimes even without the knowledge or consent of the app users. Key government officials, such as the Secretary for Security of Hong Kong and the Privacy Commissioner, were included in the DU Caller database. This incident is reminiscent of the three mobile apps that came to the attention of the PCPD in November 2016, which also involved a "reverse look-up" feature and the collection of users' contact lists[2]. Whilst the operators of the mobile apps and DU Caller app are not based in Hong Kong, and therefore do not fall within the jurisdiction of the PDPO, the individual app users residing in Hong Kong may still fall foul of the PDPO. Unsuspecting individuals would have provided their names and phone numbers to the relevant app user in order for them to store their details in their mobile device, for enabling the app user to contact them. Such individuals are unlikely to have been aware of, or to have consented to, any transfer of their name and phone numbers to the app developers.

1.1.4. *Takeaway points*

Personal data collected in a social context may be subject to the provisions of the PDPO. While the risk of complaints being filed by affected data subjects against an individual as a data user is low if the data user is an acquaintance, friend or member of one's family, the opportunity to use the privacy law as a bargaining chip in a family feud or dispute will not be lost on some.

2. India

Stephen Mathias *(Partner), Kochhar & Co.* (stephen.mathias@bgl.kochhar.com).

2.1. *CERT flexes its muscles on breach notifications*

Indian law recognizes the Indian Computer Emergency Response Team ("**CERT**") as the agency empowered to deal with cyber security. The government has also issued rules relating to cyber security incidents. The rules are unfortunately not well written, leading to much confusion. The rules state that a party "may" notify the CERT in case of cyber security incidents. The rules then go on to state that one must mandatorily notify the CERT as early as possible to leave scope for action. Read literally, it would appear that breach notifications are voluntary.

[1] See our article: "Do Not Disturb! Convictions for breach of the Direct Marketing Restrictions and Unsolicited Electronic Messages Ordinance": https://www.mayerbrown.com/files/Publication/98f5a31d-b5f1-4333-abb4-db11fefdf564/Presentation/PublicationAttachment/90274712-8db3-419a-a123-c128c4da060b/170323-ASI-IP-TMT-QuarterlyReview-2017Q1.pdf.

[2] See our article: "Dodging your call: Collection of Contact Lists by Mobile Apps":https://www.mayerbrown.com/files/Publication/4e76421b-7c12-4d24-afe4-620ce0a41b34/Presentation/PublicationAttachment/7e947d52-0a47-4544-b2da-babaf665e476/161222-ASI-IP-TMT-QuarterlyReview-2016Q4.pdf.

Please cite this article in press as: Gabriela Kennedy, Asia Pacific news, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.07.002