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** *(Associate), Mayer Brown JSM (karen.hf.lee@mayerbrownjsm.com).*

1.1. *Rectification of a data privacy breach not enough to stop an investigation*

On 2 April 2015, the Administrative Appeal Board ("**AAB**") issued a decision requiring the Hong Kong Privacy Commissioner ("**PC**") to continue investigating a data privacy complaint that it had discontinued, even though the relevant breach had already been rectified.[1]

1.1.1. *The facts*

In October 2013, an individual lodged a customer complaint with Wilson Communications Ltd ("**Wilson**") demanding monetary compensation in relation to a mobile phone he had purchased from them. The customer sent 3 letters to Wilson setting out his complaint and demanding compensation ("**Letters**"). On 27 and 28 November 2013, the customer protested outside one of Wilson's stores. In an attempt to try and protect its reputation and show the disproportionate nature of the customer's protest and complaint, Wilson publicly displayed the Letters in its shop window.

The customer lodged a complaint with the PC on the basis that the Letters contained his personal data, and was disclosed by Wilson in breach of Data Protection Principle 3 ("**DPP 3**") of the Hong Kong Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**").

On 14 April 2014, the PC notified the customer and Wilson that it had decided not to proceed with an investigation on the basis of Sections 39(2)(ca) and (d) of the PDPO:

> "*(ca) the primary subject matter of the complaint, as shown by the act or practice specified in it, is not related to privacy of individuals in relation to personal data; or*
>
> *(d) any investigation or further investigation is for any other reason unnecessary.*"

The customer lodged an appeal with the AAB against the PC's decision.

1.1.2. *The appeal*

The two main issues that the AAB had to determine were:

(a) whether or not Wilson contravened the PDPO by posting the Letters publicly on the windows of its shop front; and

* 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.

[1] Administrative Appeal No. 23/2014 of the Administrative Appeals AAB.

http://dx.doi.org/10.1016/j.clsr.2015.07.010

(b) whether or not the PC acted reasonably in its decision not to pursue the customer's data privacy complaint.

The AAB found that the Letters did contain "personal data" under Section 2 of the PDPO, as they included the name of the customer, his signature and the details of his complaint, making it possible to identify him.

Under DPP 3, a data user (i.e. Wilson) cannot use any personal data for a new purpose (i.e. a purpose not directly related to the one for which the personal data were originally provided), without the prescribed consent of the data subject (i.e. the customer). The AAB found that the purpose of the Letters was for the customer to make a claim against Wilson; and not for Wilson to post the Letters in its store window. Therefore, by posting the Letters at the store (without the customer's prior consent), Wilson contravened DPP 3.

The AAB also found that Wilson's reasons for posting the Letters in the store window (i.e. to protect its reputation) were not valid and did not exempt Wilson from complying with DPP 3. There were alternative options that Wilson could have taken to protect its reputation, such as displaying an official statement from Wilson on its position regarding the incident.

The PC conceded during the appeal that it had incorrectly notified the customer and Wilson that the main subject of the complaint was not related to the customer's personal data privacy and an investigation was unnecessary. However, the PC went on to argue that since Wilson had already taken down the Letters from its shop window, it was unnecessary for the PC to issue an enforcement notice and so his decision not to pursue the case and open an investigation was reasonable.

The customer sought leave from AAB to bring an appeal. Contrary to the PC's argument, the AAB found that the mere fact that Wilson had subsequently taken down the Letters from its shop front did not conclude the data privacy complaint in a satisfactory manner. The issuance of an enforcement notice is only one of the powers that the PC could have exercised if he had found Wilson to be in breach of DPP 3. The PC also has the right to make recommendations to Wilson on how to ensure compliance with the PDPO in the future (Section 47(2)(b) of the PDPO).

Therefore, the AAB held that even though issuing an enforcement notice may not have been necessary in this case, it had been unreasonable for the PC to discontinue the customer's complaint. The appeal was allowed.

1.1.3. *The implications*

Before the PDPO was amended in 2012, if a data user's actions amounted to a breach of a Data Protection Principle and gave rise to a complaint, the PC did not have the right to issue an enforcement notice against the data user if the breach had already been rectified and there was no evidence that there was a likelihood for the breach to be repeated. However, since October 2012, such conditions have been removed. The PC now has the power to issue an enforcement notice, even if the relevant contravention of a Data Protection Principle has already been rectified and there is no likelihood of the breach being repeated. The enforcement notice can specify the steps that the data user must take in order to prevent any recurrence of the breach. If the data user does not take such preventative steps required under the enforcement notice, it will be in breach of the enforcement notice.

Breach of an enforcement notice is an offence and may result in a fine of HK$50,000 and two years' imprisonment, and to a daily fine of HK$1000 for any continuing offence. If an infringer, after complying with an enforcement notice, commits a breach of the PDPO on the same facts, then this constitutes an offence which attracts a fine of HK$50,000 and two years' imprisonment, without the need for a new enforcement notice to be issued.

From this recent case, it seems that despite the enhanced enforcement powers introduced in 2012, the PC is at times still willing to adopt the old approach under the previous law, i.e. if a breach has been rectified then it will not proceed with an investigation or issue an enforcement notice. However, the AAB's decision seems to make it clear that the PC is now expected to take a more hard line approach, consistent with the spirit of the Amendment Ordinance, and to exercise his powers to investigate and issue enforcement notices or recommendations, irrespective of whether or not the relevant breach has already been rectified.

Interestingly, the AAB did not cite the PC's new power to issue enforcement notices even after a breach has been remedied. Instead, the AAB relied on the PC's pre-existing right to make recommendations to a data user following completion of an investigation, under Section 47(2)(b). Either way, the message is clear – rectifying a breach of the Data Protection Principles under the PDPO may not necessarily prevent a data user from escaping scrutiny under the law, as even if the PC decides not to take any action, such decisions may be reversed by the AAB.

2. China

Xiaoyan Zhang *(Counsel), Mayer Brown JSM (*xiaoyan.zhang@mayerbrownjsm.com*);* **June Lau** *(Trainee Solicitor), Mayer Brown JSM (*june.lau@mayerbrownjsm.com*).*

2.1. *A look back on a decade of electronic signature laws in China and Hong Kong*

China's Electronic Signatures Law ("**ESL**"), first implemented on 1 April 2005, was revised by the National People's Congress on 24 April 2015 (the "**Revisions**").[2] The revisions intend to streamline the registration process by eliminating the requirement for electronic certification service providers ("**ECSP**") to obtain a license for certification services from the MIIT (Ministry of Industry and Information Technology) first *before* they can apply for its legal enterprise status with the SAIC (State Administration for Industry and Commerce).[3] After the Revisions, an ECSP can register as a legal enterprise with the SAIC first and *then* apply for a license with the MIIT. The Revisions

[2] http://www.npc.gov.cn/npc/cwhhy/12jcwh/2015-04/25/content_1934598.htm.

[3] Para. 5(2), Decision of the Standing Committee of the National People's Congress on Revising the Electric Power Law of the People's Republic of China and Other Five Laws.