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

ABSTRACT

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

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. Blood, sweat and tears: guidance issued in Hong Kong on the collection and use of biometric data

Face recognition technology to help "tag" friends in photographs, fingerprint recognition to unlock smartphones, and fingerprint door locks are just some of the ways in which biometric data have been used in recent years. The constant barrage of news of cyber-threats has sparked a renewed interest in biometrics: DNA matching, visual biometrics (retina, iris, ear, face fingerprint, hand geometry), spatial biometrics (finger geometry, hand geometry, signature recognition), auditory biometrics (voice authentication or identification), olfactory biometrics (odour), behavioural biometrics (gait, typing recognition) and biometrics based on brain and heart (drawing on certain brain and heart patterns unique to each individual) are just some of the possible technologies being discussed. In Asia, the uptake of biometric technology includes the development of palm vein authentication technology for payments in Japan, the upcoming introduction in April 2016 in Japan of Biocarts to capture fingerprints and photos of passengers to try and cut down the immigration processing time; fingerprint authentication for ATM transactions in Vietnam; and the launch of facial recognition technology for ATMs in China. Is this the end of long passwords and two-factor authentication systems and the time to give our memory a well-earned break from having to remember frequently changed passwords?

1.1.1. Biometric data – For or against?

In a consumer context, biometric technology can enhance the users' experience by speeding up delivery and allegedly offering increased security. But is a fingerprint scan more secure than traditional password authentication? Fingerprints can be easily "lifted" and used to fool fingerprint sensors to gain access to a device, as a recent incident involving a German politician has shown us.

Outside of the consumer context, there has been an increased uptake in biometric technology to track employee attendance. Such use gives rise to a number of data privacy concerns, particularly due to the nature of the employer–employee relationship where there is inevitably an unequal balance of power.

Biometrics is also attracting a lot of interest as a tool for stepping up national security in an age of hyper-sensitivity over cyber-attacks and cyber-espionage. The possible introduction of facial matching systems relying on stills rather than live

For further information see: http://www.mayerbrown.com

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong. Tel.: +852 2843 2211; Fax:+852 2103 5433.
E-mail address: gabriela.kennedy@mayerbrownjsm.com

http://dx.doi.org/10.1016/j.clsr.2015.12.011

CCTV feeds for use by law enforcement and security agencies has sparked controversy in Australia recently due to a 20% margin of error.

The fact remains that regardless of the benefits of biometrics, the collection of such sensitive data in itself makes the individual vulnerable to a different type of threat, namely misuse, theft, leakage of data or, in some situations, an erosion of human dignity. Unlike passwords, which can be reset when hacked, biometric features – when stolen – cannot be replaced.

1.1.2. *Closer to home – Hong Kong*

In Hong Kong, the biggest collector of biometric data is the Hong Kong government. All Hong Kong residents have their finger print data stored on their Hong Kong identity cards. A new smart biometric identity card, for which the Hong Kong government has set aside a whopping budget of HK$ 2.9 billion, is expected to be introduced in phases between 2018 and 2022 and will store higher resolution images for facial recognition and enhanced biometric data.

There is also an increasing adoption and use of biometric technology amongst businesses in Hong Kong. This, as well as a few recent instances of misuse of biometric data, raised concerns with the former Hong Kong Privacy Commissioner (“**PC**”), especially in an employment context. On 20 July 2015, the outgoing PC, just days before completing his term in office, issued a Guidance on Collection and Use of Biometric Data (“**Guidance Note**”).[1]

1.1.3. *Sensitive data and biometric data in the Hong Kong context*

Even before the issuance of the recent Guidance Note, and despite there being no separate definition of “sensitive data” under the Personal Data (Privacy) Ordinance (“**PDPO**”), the previous PC tended to take a stricter approach on the application of the Data Protection Principles (“**DPPs**”) under the PDPO in respect of personal data that he considered to be “sensitive”, taking into account the nature of the information (see various guidance notes and reports of investigations issued and conducted by the PC in the last couple of years). Some examples of personal data that are generally considered to be “sensitive” data include Hong Kong identity card numbers, medical records and biometric data.

During the consultation period for the Amendment Ordinance 2012 (which introduced changes to the PDPO), the government considered introducing a new category of “sensitive data” (which included biometric data) with more stringent controls attached. Due to a lack of consensus on the coverage and regulatory model for the protection of sensitive data, the proposal was not pursued.[2] We note in passing that many representatives from the information technology sector strongly opposed the proposal lest it would hamper the development of biometric technology.[3] While the proposal to introduce a new regime to protect “sensitive data” and, particularly, biometric data was set aside, the government suggested that the PC issue guidelines on best practices on the handling of biometric data, in order to afford better protection to individuals.[4]

On 20 July 2015, the Guidance Note[5] was issued in the wake of several cases that raised public concern on the collection of DNA and fingerprints by employers. This was almost the swan song for the former PC before his term finished on 3 August 2015. The Guidance Note replaces the Guidance Note on the Collection of Fingerprint Data issued in May 2012.

1.1.4. *Bits of us: Hong Kong cases relating to biometric data*

One of the cases that prompted the issuance of the Guidance Note concerns an investment company, which in May 2014 made headlines when it required all female staff to provide blood samples for DNA testing in a misguided attempt to investigate toilet hygiene complaints. On 21 July 2015, the former PC issued an investigation report regarding the collection of employees’ fingerprint data by a fashion trading company. In both cases, the former PC found that the collection of such data was excessive, as the sensitive nature of the data was disproportionate to the purpose of collection, and less privacy intrusive measures were available.

In an employer–employee context, even if the collection of biometric data may be justified and proportionate, alternative options should still be provided to the employee (e.g. choice of password access instead of fingerprint scan), otherwise the employees’ consent on the collection and use of their biometric data cannot really be said to be voluntary or “fair” for the purposes of the PDPO.

1.1.5. *Guidance Note*

The Guidance Note (which is reminiscent of the EU Biometric Opinion) provides practical guidance to data users on the limited circumstances when biometric data may be collected and, if it can be collected, the steps that need to be taken regarding the collection and storage of such data, namely:

(i) biometric data should only be collected and used in accordance with the relevant data privacy law;
(ii) there must be a clear legal purpose for which the biometric data is being collected;
(iii) biometric data must only be collected and used if it is relevant and not excessive in order to achieve such purpose;
(iv) an analysis should be conducted to determine whether the proposed biometric technology is essential to and will be effective to achieve the relevant purpose, and whether there are less privacy intrusive alternatives;
(v) sufficient and effective security measures should be implemented to protect the biometric data, taking into account the sensitive nature of the data; and
(vi) the data user should establish a retention period, and should ensure that biometric data is deleted once it is no longer needed for the purpose in which it was collected.

[1] https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

[2] The Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance issued in October 2010 by the Hong Kong government: http://www.cmab.gov.hk/doc/issues/PCPO_report_en.pdf

[3] Ibid 2.

[4] Ibid 2.

[5] https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf