available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia-Pacific news

Gabriela Kennedy

Hogan Lovells, 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

1.1. *Privacy Commissioner publishes Guidance Note and model notification form to data users on handling breaches of personal data privacy*

On 21 June 2010 Mr. Roderick Woo, the Privacy Commissioner of Hong Kong, issued the "Guidance Note on Data Breach Handling and the Giving of Breach Notifications" (the **"Guidance Note"**), intended to be used by data users to establish best practices in handling breaches of personal data.

1.2. *Background*

Like equivalent legislation in other Asia-Pacific jurisdictions, the Personal Data (Privacy) Ordinance (the "**Ordinance**") does not require data users to notify any authorities or data subjects of a breach of the personal data held by it. As part of the review of the Ordinance undertaken by the Constitutional and Mainland Affairs Bureau ("**CMAB**") from 2007 to 2009, CMAB recommended that the Government amend the legislative framework to implement a voluntary breach notification system. This would allow the Government the opportunity to assess the impact of breach notifications and ensure that the regulatory requirements and reasonable and practicable.

Throughout the review process, the Privacy Commissioner has consistently advocated a breach notification system be adopted, under which data users are required to adopt a containment plan in the event that personal data privacy is compromised, and in certain circumstances data notify the data subjects of the security breach. Although the proposals of either CMAB or the Privacy Commissioner are yet to be adopted in the private sector, the Government has in the meantime implemented a scheme requiring public organisations to notify both the Privacy Commissioner and the affected data subjects of any electronic personal data leakage.

1.3. *The Guidance Note*

The Guidance Note is intended to provide "good policies and practices" for data users to take remedial action to contain and mitigate the damage caused by personal data leakages. In the Commissioner's view, prompt and effective action will not only allow data subjects to take appropriate measures on learning of the breach of their personal data, but will assist data users to avoid the risk of litigation action and to restore reputation and public confidence.

The Guidance Note sets out what constitutes a data breach and sets out how a data breach should be handled by the data user, from gathering information relating to the breach, containing the breach, assessing the risk of harm to data subjects, to considering whether the data subject should be notified. Finally, the Guidance Note sets out how notification should be given and the rationale behind a regime of notification.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2010.08.002

1.4. *Data breaches in Asia*

On 3–4 June 2010, the Privacy Commissioner represented Hong Kong at the Asia-Pacific Privacy Authorities Form, where the issue of data breach notification was discussed at length. All of those present agreed that data notification is an important practice for data users to adopt, and discussed the development of a template notification form by regulators for data users to use when notification to a regulatory body (such as the Commissioner) is called for. As a result of the discussions and the developments discussed above, the Commissioner has prepared a template for Hong Kong data users to use, which is available on the Privacy Commissioner's website (www.pcpd.org.hk).

Gabriela Kennedy *(Partner) (gabriela.kennedy@hoganlovells.com) and* **Olivia Lennox-King** *Stewart, Hogan Lovells, Hong Kong.*

2. Australia

2.1. *Government releases draft of new privacy principles*

2.1.1. *In brief*

- The release of an exposure draft of a new set of privacy principles, to be known as the Australian Privacy Principles, represents the first stage of public consultation in relation to the proposed revision and restructuring of Australia's privacy legislation.
- The Australian Privacy Principles are intended to replace the existing Information Privacy Principles (which apply to Commonwealth agencies) and the National Privacy Principles (which apply to certain private sector organisations).

On 25 June 2010, the Australian government released an exposure draft of a new set of privacy principles, to be known as the Australian Privacy Principles (APPs).

This initiative represents the first stage of public consultation in relation to the proposed revision and restructuring of Australia's existing privacy legislation. It has been foreshadowed that there will be subsequent consultation in relation to legislative reforms affecting credit reporting information, health information and the functions and powers of the Australian Information Commissioner.

Once each of these components has been examined by a Senate Committee, a new Bill will be consolidated and introduced into parliament. No time frame for the completion of this process has been announced.

2.2. *Objective of new principles*

The APPs are intended to replace the existing Information Privacy Principles (which apply to Commonwealth agencies) and the National Privacy Principles (which apply to certain private sector organisations), thereby addressing one of the major structural incongruities of the *Privacy Act* as identified by the Australian Law Reform Commission in its 2007 report. The other structural incongruity, being separate privacy principles applicable to certain State and Territory Governments, would appear to be set to continue for the foreseeable future.

2.3. *Terminology*

In some instances, the application of the new principles continues to be restricted to just "agencies" or "organisations" but for the most part they apply to both which are generically described as "entities".

The exposure draft also refers to the "Commissioner" in a generic sense. Under the current *Privacy Act*, this can be taken as a reference to the Privacy Commissioner but following the commencement of the *Freedom of Information (Reform) Act 2010* and the *Australian Information Commissioner Act 2010* (principally on 1 November 2010), these references will be taken to mean the Australian Information Commissioner.

2.4. *Structure*

The new APPs are set out in Part A of the exposure draft. Part B deals with other relevant provisions.

APPs 1–2 deal with the responsibility of entities to establish appropriate infrastructure and practices relating to privacy. APPs 3–5 deal with the collection of personal information and APPs 6–9 address the responsibilities of entities in handling personal information. APPs 10 and 11 address the need to maintain the quality and security of personal information under an entity's control, and APPs 12 and 13 deal with rights of access and correction.

The sequencing of the APPs is intended to reflect the logical cycle in which entities collect, hold, use and disclose personal information.

2.5. *The new principles*

The general thrust of the new principles – which digress in a number of respects from those recommended by the Australian Law Reform Commission – is discussed below.

2.5.1. *APP 1 – open and transparent management of personal information*

APP 1 requires entities to manage personal information in an open and transparent way. An entity must take reasonable steps to ensure that practices and procedures relating to its functions and activities will comply with the APPs. An entity must have a privacy policy describing what information is held and how it may be accessed, and the policy must to the extent practicable specify any overseas recipients to whom such information may be disclosed.

2.5.2. *APP 2 – Anonymity and pseudonymity*

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity unless it is unlawful or impractical to do so. According to the Companion Guide issued by the government, the Commissioner will be encouraged to provide guidance on the types of circumstances in which it will not be "lawful or practical" to provide this option.