*University of New South Wales Law Research Series*

# THE LEGAL AND BUSINESS RISKS OF INCONSISTENCIES AND GAPS IN COVERAGE IN ASIAN DATA PROTECTION LAWS

**GRAHAM GREENLEAF**

Session II Materials, Asian Business Law Institute (ABLI) Data Privacy Forum, Singapore, 7 February 2018
[2018] *UNSWLRS* 10

UNSW Law
UNSW Sydney NSW 2052 Australia

**E:** unswlrs@unsw.edu.au
**W:** http://www.law.unsw.edu.au/research/faculty-publications
**AustLII:** http://www.austlii.edu.au/au/journals/UNSWLRS/
**SSRN:** http://www.ssrn.com/link/UNSW-LEG.html

# ABLI Data Privacy Forum

## Session II. The legal and business risks of inconsistencies and gaps in coverage in Asian data protection laws

The issues in this Session are seen from the perspective of a company conducting business in on or more Asian economies, or a foreign business intending to export personal data to one or more Asian economies for further processing (including intra-company transfers).

What difficulties do inconsistencies/gaps between Asian data privacy laws present for their understanding /complying with these laws? The lists below show some of the main areas where such problems arise, and attempt to give a brief explanation of the nature and extent of 'gaps'. Jurisdictions mentioned are not comprehensive, but indicate the range of options (ie gaps) found in Asian laws. Areas where all jurisdictions' laws are similar and there are not significant gaps (eg forms of data covered; rights of access and correction) are not mentioned.

These examples do not cover inconsistencies/gaps in relation to cross-border cooperation (Session III), data localisation (Session IV), data transfer mechanisms (Session V), or enforcement mechanisms.

Details of all gaps referred to here can be found in my publications.*

– *Graham Greenleaf, 7 February 2018*

## Some gaps in scope and coverage

### Definitions of 'personal information' / 'personal data'

All laws are based on 'personal information' (or data) defined by the capacity of information to identify a person ('identifiability'). Japan and Korea exempt completely information from which a person is not 'easily'/'readily' identified. Hong Kong's requirement that information must be collected with an 'intention to identify' has had little practical effect.

### 'Anonymised' / 'de-identified' data

Japan's law exempts from normal principles 'anonymous process information' (API), as defined in the Act, but imposes a separate set of principles on API. Korea's 'Big data guidelines' (not its laws) purport to do something similar. In other jurisdictions, the extent to which processing of personal data for purposes of 'de-identification' is allowed (or even required) is not explicitly stated, and nor is its effect on removing such data from the scope of the law.

### Exemption of publicly available data

Do data privacy laws apply to personal data which has become publicly available? At one pole (similar to the EU), Hong Kong's law does apply, including to data in government 'public registers' (unless specific rules state otherwise), and Korea and Macau are similar. At the other pole, Singapore, New Zealand and Australia explicitly exempt publicly available data; Taiwan and Malaysia may impliedly do so. Japan exempts data compiled legally and sold to or purchasable by ' a large number of unspecified persons', or provided unaltered for its original purpose.

---

* See G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP 2014), particularly chapter 17 'Comparing Protections and Principles', and *2014-17 Update* at <https://papers.ssrn.com/abstract_id=3000766>

### Exemptions for certain 'non-commercial' activities

While all Asian laws exempt personal data used for personal, household and family affairs, there are a wide range of jurisdiction-specific exemptions for types of supposedly 'non-commercial' activities, including activities of clubs and voluntary associations (common), religious/missionary activities (Japan, Korea), political parties (Australia, Korea, Japan), and even everything non-commercial (Malaysia, India – 'corporations' only).

### Exemptions for 'small' businesses (or SMEs)

Most laws apply to all businesses/data controllers, but Australia exempts 'small' businesses based on turnover (over 90% of businesses). Japan's pre-2015 law exempted databases with less than 5000 individuals (an indirect SME exemption), but does not now do so.

### Subject-based exemptions

Exemptions based on the subject-matter of the personal data are common, including in relation to defence, national security, international relations, criminal investigations, legal proceedings, legal professional privilege, protection of mental or physical health, and research and statistical uses. There is relatively little consistency between jurisdictions in the scope of exceptions, or method of expressing exceptions. Singapore has exceptionally long and complex schedules of exemptions. The extent of problems they cause for businesses, or data subjects, is uncertain.

### News media and freedom of speech exemptions

Unlike Europe, Asia has no binding international treaties with freedom of speech requirements against which data privacy laws must be balanced, and only about half of the jurisdictions in Asia have constitutional rights of freedom of speech. Consequently, while most Asian data privacy laws make some attempt at balance, the range of responses varies widely, with the differences most often being found between jurisdictions where free speech has a constitutional foundation and those where it does not. Summary is not possible here.

### Relationship between sectoral laws and principal data privacy law

Whole sectors of an economy are rarely completely exempted from a country's main data privacy law. Malaysia's complete exemption of credit reporting agencies, which have a separate law, is unusual. More common is that special sectoral laws covering data privacy apply to particular sectors, as well as the general data privacy law, with the relationship between the special and general laws being either uncertain or complex (eg Korea's special laws concerning network services, and financial services), particularly for foreign businesses relying on translations. 'What do we comply with?' is a common complaint.

### Parties regulated, and their liabilities: 'controller', 'processor' etc

From both the business perspective ('are we liable?') and the individual perspective ('who is liable to me?') the differences between jurisdictions in relation to controllers and processors are important gaps. In Hong Kong, Singapore and Malaysia, obligations are essentially imposed on controllers only, with very limited imposition on processors, for security and sometimes destruction after use. In contrast, Korea, Taiwan, and Macau impose all obligations on processors as well. So does the Philippines, except for processing foreign-sourced data. Considerable complexity is added by varying laws on when controllers are vicariously liable for the acts of processors (and whether they are acting within or outside their authority).

Half of India's principles only apply to 'sensitive' information, and half only apply to 'providers' of information (not data subjects), making the law inapplicable in numerous (non-definable) situations.

### 'Outsourcing' exemptions

Lower standards of protection (or none at all) may apply to data being processed on behalf of an overseas controller (an 'outsourcing exemption'). This is explicitly so in the Philippines, and implied in different ways in Hong Kong, Singapore, Malaysia and Vietnam. It is not so in other jurisdictions. Outsourcing exemptions may be attractive to businesses processing data for US companies, but may result in extra compliance burdens on companies wishing to process data from the EU (or any other jurisdictions with data export restrictions).

### Extraterritorial scope

Some Asian laws may have extraterritorial application where equipment in the jurisdiction is used for processing by an overseas party. This is unusual but could sometimes occur in Macau, the Philippines or Singapore.

### Boundary of public and private sectors

While most Asian laws are comprehensive of both private and public sectors, Asia is unique in its number of private-sector-only laws (Singapore, Malaysia, Vietnam, India). Singapore also exempts any business if they are working for the Singapore government (how do you know?).

## Some gaps in relation to processing

### 'Minimal' collection

Most Asian jurisdictions (Hong Kong, Macau, Korea, Taiwan, Japan, Singapore, Australia, New Zealand) implement the stricter approach of 'minimal' collection (that personal data should only be collected where necessary for a specified purpose), as in the EU. A minority of jurisdictions (Malaysia, Philippines, Vietnam by implication), allow collection that is 'not excessive', the more permissive OECD approach.

### Notice at time of collection

All jurisdictions require notice of purpose and other matters to be given to the data subject at the time of collection (or at least before first use), except the Philippines and Japan (exception where purpose has been disclosed in advance). However, the specificity of the content required in such notice varies a great deal, particularly where data export is intended. Notice to the data subject when data is collected from 3rd parties is only explicitlyu required in Korea, Macau and Taiwan.

### Requirements for valid consent (where consent is the basis of processing)

While consent to processing may be implied from notice in some jurisdictions, in others it must be express consent, though this is described in various ways: 'unambiguous' (Macua); written (Taiwan); standard form (Indonesia); 'evidenced' (Philippines); written 'prescribed' consent (Hong Kong). Korean consent requirements are the most strict: 'unbundling' of each item requiring consent, and segregation of items requiring consent from those that do not.

### Permitted bases for secondary uses

All Asian laws implement the principle of 'finality' (that subsequent use and disclosure is limited by the original purpose of collection) to some extent. In almost all jurisdictions, such secondary uses are allowed if they are compatible / 'not incompatible' with the purpose of collection, though wordings differ considerably. A few laws apply different tests: New Zealand and Malaysia require secondary uses be 'directly related'; Singapore has a 'reasonable person' test, and Japan a 'reasonably relevant' test (all with many exceptions).

All jurisdictions then add exceptions for non-related uses to the basic secondary uses test, including some for the protection of the legitimate interests of others (Macau, Philippines). Exceptions based solely on notice of non-related uses are not allowed, except for disclosures (not internal uses) in Japan.

### Direct marketing restrictions

Seven regional laws include the right to opt out from direct marketing (Macau, Malaysia, Taiwan, Vietnam, Australia), with Hong Kong and Korea going further and requiring consent (ie opt-in) at collection if data is to be used for marketing purposes. There is a gap with those countries (Singapore, Malaysia, Philippines, Japan, New Zealand) with no such requirements.

### Additional protections for 'sensitive' data

Many countries provide some additional protection to defined categories of 'sensitive' data (Australia, Japan, Korea, Macau, Malaysia, Philippines, Taiwan) but the categories vary a great deal, often being a sub-set of the EU categories. At the other pole, the Philippines adds extra categories to those familiar in the EU. Very important categories such as genetic and biometric information have very wide variations in definition and inclusion. In each jurisdiction, the protections consequent upon a classification as 'sensitive' differ greatly, usually starting with more strict consent requirements (eg Korea requires unbundled consent), perhaps including more limits on disclosure (Japan).

Other countries have no such projections in their general law (Singapore, New Zealand, Hong Kong, Vietnam, China) but often have some in sectoral laws (eg old criminal records; ID numbers). India's provisions do not provide additional protection, because 'non-sensitive' data has no protection. These 'gaps' in definition and administration are both harmful to data subjects and dangerous to businesses that will find it difficult to be aware of them across jurisdictions.

### Deletion/ de-identification requirements

Most countries require that personal data be deleted or de-identified after its use is completed (Australia, Hong Kong, Japan, Korea, Macau, Malaysia, Philippines, New Zealand, Taiwan, Singapore, Vietnam), or after a specific period (Indonesia). There is often ambiguity concerning whether de-identification is sufficient. The gap here is only with China and India.

### Notifications of corrections

Most Asian jurisdictions require 3rd parties who have accessed a person's file to be notified of corrections to that file (Hong Kong, Singapore, Macau, Taiwan, Philippines, and Macau), with Korea leaving the decision to notify to the data subject.

### Data breach notifications

Data breach notifications (DBN) are required by law: to individuals likely to be affected (Korea, Philippines, Taiwan, Australia, Indonesia); to data protection authorities (China, Philippines, Korea, Australia). Other jurisdictions are actively considering introducing DBN (Singapore, New Zealand).

### New gaps are likely in future

It is likely that new types of 'gaps' will arise between Asian laws in the near future, as technological developments and global advances in data protection (particularly the EU GDPR) have continuing effects on Asian jurisdictions. For example, some Asian jurisdictions have already enacted 'right to be forgotten' laws (Indonesia), data portability (Philippines), some limits on automated processing (Macau, Philippines and New Zealand), and additional restrictions on some sensitive processing systems (notification; 'prior checking' by DPA etc) (New Zealand, Philippines).