Limitations of Malaysia's data protection Bill

Graham Greenleaf, University of New South Wales Faculty of Law
For publication in *Privacy Laws & Business International Newsletter* Issue 104, April 2010

The *Personal Data Protection Bill 2009* expected to be enacted by Malaysia's Parliament this April will add a distinct new flavour to Asia's growing array of data protection laws. The Bill has been outlined by Abu Bakar Munir (PLBI Newsletter Issue 102, December 2008, p18). This article concentrates on the limitations of the Bill that may prove to be impediments to effective data protection, and on its influences and novel aspects.

Scope limitations

The Bill applies only to personal data in 'commercial transactions' (s2), though they are defined broadly ('includes any matters relating to the supply or exchange of goods or services': s4). Credit reporting agencies are exempt and will be subject to separate legislation (also expected to be tabled in April). There is the usual exemption for 'personal, family and household affairs' (s45(1)), but the limitation to 'commercial transactions' will also exclude the non-commercial affairs of churches, educational institutions and non-profit organisations. There is no 'small business exemption', unlike in Australia or Japan.

Processing for the purpose of publishing 'journalistic, literary or artistic material' is exempted (except from the Security Principle), but only where the data user reasonably believes that (a) the publication would be in the public interest (taking into account the 'special importance of public interest in freedom of expression'), and (b) compliance with a particular Principle or provision is 'incompatible with the journalistic, literary or artistic purposes' (s45(2)(f)). This is not a blanket 'media exemption' but a carefully written partial exemption, and one which will be complex for the media, Commissioner and courts to apply. It is important that this Act should not unduly restrict freedom of expression in Malaysia.

There is a very broad exemption for any processing by commercial organisations 'for the purpose of discharging regulatory functions' where application of the Act would be likely to prejudice those functions (s45(2)(e)), and other broad exemptions for prevention of physical or mental harm, for statistical and research uses that do not produce identified outputs, and in connection with court processes. These are not blanket exemptions from all Principles, and typically do not provide exemptions from the Security, Data Integrity and Retention Principles. In addition, there are lengthy lists of exemptions from specific Principles, particularly Disclosure.

The largest omission is that the public sector is not covered at all (s3(1)). Malaysia has no existing protections for personal information which limit State abuses of privacy.

This Bill can only be said to cover part of the private sector, and only then subject to many exceptions, particularly where any State-related activities are concerned. Within its scope it may still be valuable, but the narrow scope must always be kept in mind.

A Commissioner but little independence

Malaysia will have a Personal Data Protection Commissioner appointed by the Minister (s47), with a normal range of powers. The Commissioner will be appointed for up to three

years, and may be re-appointed (s53), but he or she may also be dismissed by the Minister, who only needs to 'state the reason' (s54). The Commissioner's remuneration and allowances are also determined by the Minister (s57). The Commissioner's annual report goes to the Minister (s60), with no requirement that it goes the Parliament or be made public. In order to further underline the Commissioner's lack of independence, it is explicitly stated that 'the Commissioner shall be responsible to the Minister' and 'the Minister may give the Commissioner directions of a general character consistent with the provisions of the Act' (s59). However, the Commissioner is protected against legal actions while carrying out his or her duties in good faith (s139).

A Commissioner who is not independent may still be effective, at least while he or she has a Minister sympathetic to privacy. But there is no point pretending that this Commissioner's office is like that of other Privacy Commissioners in the Asia-Pacific. Those in Australia, New Zealand, Canada and Hong Kong have statutory provisions underwriting their independence which are not found here. The international Data Protection Commissioners have established accreditation requirements which require that a Data Protection Authority has 'an appropriate degree of autonomy and independence'. The notes to that requirement refer to such matters as ability 'to operate free from political or governmental interference' and 'removal only for inability to perform the office, neglect of duty or serious misconduct'. The Asia Pacific Privacy Authorities (APPA) meeting requires members to be accredited to the international conference. It would be embarrassing if the Malaysian Commissioner could not even attend regional Commissioner's meetings as a full member, or global meetings.

Seven Principles and some additional ones

The seven Personal Data Protection Principles in the Bill's ss5-12 (General; Notice and Choice; Disclosure; Security; Retention; Data Integrity; and Access) are influenced strongly by the EU data protection Directive rather than by the OECD Guidelines or APEC Framework. The EU-style starting point is that processing of personal data (including collection) requires consent (s6), subject to the many exceptions in s40.

The EU Directive's influence is seen even more clearly in a number of additional principles (details of which are in Munir's article): the right of data subjects to withdraw consent to processing (s38); a further right to prevent processing likely to cause damage or distress (s42), which is independent of questions of consent; and the right to prevent processing for the purposes of direct marketing (s43).

The Principles have possible weakness in the limits on use and disclosure. Data users must obtain data subject consent to processing of their data (s6). They must give 'written notice' of the purpose of collection (s7) no matter how the data is collected. They need not give it at the point of collection, if not 'practicable', but must give it before use for related purposes or disclosure (s7(2)). Data may only be used for purposes 'directly related' to the purpose of collection (s6(2)).

Companies can effectively negate the limitation on disclosures to purposes 'directly related' to the purpose of collection (s8(a)) simply by disclosing 'the class of third parties' to whom they may disclose the data (s7(1)(e) and s8(b)). Is this a blank cheque for Malaysian companies to disclose personal data to anyone they choose, provided they make a vague statement about the possibility of such use in a written notice? The position is more complex than that, because the recipient would still have to have the data subject's consent to process the data, or be able to rely on one of the exceptions allowing processing (s6).

The processing of sensitive personal data (which has a broad definition including allegations of commission of offences) requires 'explicit consent' (which suggests that 'consent' by itself includes implied consent), or for other exceptions to apply (s40). Among the list of very broad exceptions are that the use is necessary 'for the exercise of any functions conferred on any person by or under any written law' or 'for any other purpose as the Minister thinks fit'. There is also an exception where a person has made public their own sensitive personal data (s40(2)), which is not an exception for ordinary personal data. There is a real danger with this provision that it will be abused by the Malaysian state (which is in effect exempt from the legislation) whereas those who attempt to raise allegations of criminality or discuss other sensitive issues could be prosecuted if they fall outside the media exemptions. The provisions are complex, but the danger is there.

The Security Principle (s9) is weak, in that it only requires data users to 'take practical steps', not 'take reasonable steps' as is often required, but whether this amounts to any real difference remains to be seen.

Extra-territoriality, 'whitelists' and due diligence

The Act will have no application to processing outside Malaysia, with the interesting exception of where data is intended to be further processed in Malaysia (cl 3(2)). Temporary exports of data from Malaysia for purposes of processing breaching the Act will therefore be subject to it. It applies to anyone 'established in Malaysia' or who uses equipment in Malaysia.

Personal data may not be transferred outside Malaysia unless the destination is on a 'whitelist' specified by the Minister, after receiving the Commissioner's advice (s129). The Minister can so specify a place if it has in force a law 'substantially similar' to the Malaysian Act, or the place ensures 'an adequate level of protection … which is at least equivalent to the level of protection' provided by Malaysia's Act. There are exceptions similar to those found in Article 26 of the EU data protection Directive, but some which go considerably further than the Directive, including where 'the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in a manner which, if that place is Malaysia, would be a contravention of this Act' (s129(3)(f)).

Unless the Commissioner takes a strict interpretation of when a data user has 'taken all reasonable precautions and exercised all due diligence', s129 will involve a front door to data exports (the 'whitelist') which appears to be shut, while the back door is wide open to transfers to anywhere, with exporters absolved from any accountability for what goes wrong.

Worthless remedies?

Data users who breach one of the Principles commit an offence carrying substantial fines or even imprisonment (s5(2)). If the Commissioner, after investigation, considers that a data user is contravening the Act or has done so and is likely to continue or repeat doing so, then the Commissioner can issue an enforcement notice requiring the contravention to be remedied (s108). Substantial fines can result from failure to observe enforcement notices. There is a right of appeal against issuance of an enforcement notice to an Appeal Tribunal (Pt VII). There is no right of appeal against non-issuance of an enforcement notice, which is unfair to data subjects, and surprising since there is a right of appeal against the Commissioner's failure to investigate a complaint (s93).

As with the Hong Kong law, this reliance on enforcement notices has the fatal flaw that breaches that have caused harm, but are unlikely to be repeated, fall outside the scope of the Act. This is coupled with the other fatal flaws that there is no obvious way by which complainants may seek compensation for damage: the Commissioner cannot award damages; data subjects cannot take seek compensation in court (which they can in Hong Kong, in theory).

The Commissioner has powers to inspect data user's systems (s101), but overall the 'enforcement pyramid' in this Act is completely deficient. No matter how diligent a privacy Commissioner may be, if they do not have the necessary enforcement tools, there are severe limits to what they can achieve. The Commissioner needs more arrows in the quiver than this Bill provides.

Will there be registration and codes?

Registration of specific classes of data users may be required by the Minister on the recommendation of the Commissioner (s14). The Commissioner can also designate a body (such as an industry association) as a 'data user forum' (s21), which is then able to prepare a code of practice (s23), which the Commissioner may then issue (s24). Data users belonging to that class must then comply with this code (s25), with breaches subject to substantial fines (s29). Whether these procedures see any use remains to be seen. While both could be useful, used sparingly, experience in other jurisdictions has not shown them to be important as yet.

A modest step forward for Malaysia

While this Bill has many deficiencies, privacy legislation even of these modest dimensions will be a step forward for Malaysians. In the hands of a Commissioner committed to privacy protection, much will still be able to be achieved. If the Act is well managed, Malaysian politics may deliver further improvements to it in future. For Malaysians to be able to focus on real issues in data protection will inevitably increase the demand for better protection.