Twenty-one years of Asia-Pacific data protection

Graham Greenleaf, Asia-Pacific Editor

Published in *Privacy Laws & Business International Newsletter*, Issue 100, August 2009, pgs 21-24

The twenty-one years since *Privacy Laws & Business* commenced publication coincides almost exactly with the development of data protection in Asia and the Pacific (the Americas are a separate story). It is therefore an appropriate opportunity to take a chronological overview of how information privacy or data protection laws in this part of the world have developed while PL&B was obtaining maturity. Of course this only gives part of the picture, because constitutional rights and general provisions of civil and criminal laws may also protect privacy.

The slow growth of data protection laws

There are seven jurisdictions in the region which have enacted data protection laws. As yet, the European Union has not declared whether any of their laws are 'adequate'.

Australia's *Privacy Act 1988* (Cth) only covered its federal public sector, but was the first law in the region to enact a full set of Information Privacy Principles (IPPs), based on the OECD Guidelines, and establishing an office of Privacy Commissioner. The Act was expanded in 1991 to cover credit reporting, and finally in 2001 to include the private sector, but with notable very large exceptions for employment records, for so-called 'small business operators' (defined broadly enough to exempt about 90% of all Australian businesses), political activities and media activities. The Act has relatively strong enforcement provisions, but an unwillingness to use them by a series of Privacy Commissioners, and the absence of any provisions for complainants to appeal to the Courts, has resulted in only a handful of 'determinations' by the Commissioner, and one significant Court decision, after twenty-one years. So Australia's federal privacy law is still largely unknown territory, and agencies and companies can treat its more difficult provisions as optional in the absence of any evidence to the contrary. Almost all of Australia's States and Territories now have data protection laws for their public sectors, some with more effective enforcement through administrative Tribunals.

Japan has had an *Act on the Protection of Personal Information Held by Administrative Organs* governing public sector data since 1988, but it was strengthened to cover paper-based files and penalties for disclosures in 2003. *The Act on the Protection of Personal Information* provided the first coverage of the private sector in 2003. There are confusing exemptions for 'small business' based on the number of persons covered by their databases, for the media and others. The OECD-influenced principles in the 2003 Act are unexceptional, but their meaning is to a large extent determined by 24 different sets of Ministry guidelines aimed at different sectors. There is no central enforcement body. The Act has been held not to create a private right of action before the Courts, so complainants are left to the mercy of enforcement and mediation by relevant Ministries. There is no evidence of effective Ministerial supervision. Although consumer centres and government receive over 12,000 complaints per year, only a handful of complaint summaries are published, and evidence of the Act's effectiveness is lacking. The Act

provides a formal role for 'authorized personal information protection organizations' (APIPO) to help resolve complaints in some way, but how they do this is obscure. The effect of the self-regulatory PrivacyMark system is equally enigmatic.

New Zealand's *Privacy Act 1993* was the region's first comprehensive law governing both public and private sectors and establishing the office of Privacy Commissioner. Its twelve information privacy principles (IPPs) are substantially based upon on the OECD Guidelines with some Australian influences. It is probably the most effectively enforced law in the region. Most of the approximately 650 complaints per year received by the Commissioner are closed within the year of receipt, many resulting in agreed settlements. However, around twenty per year are referred to the Human Rights Review Tribunal (HRRT), which has powers to make enforceable orders and often does so. The highest damages awarded has been NZ$40,000, followed by NZ$20,000. There are numerous damages awards for wrongly collecting information, poor security safeguards, wrongly denying access, holding inaccurate information on a database, and wrongful disclosure of information. There are rights of appeal to the High Court, which has heard twenty three such cases, and to the Court of Appeal which has heard one. As a result of around 200 such HRRT and Court decisions, New Zealand has rich body of privacy law, and an Act where complainants and respondents alike can understand the consequences of breaches. It is now proposing to remedy its weakest aspect, lack of a data export restriction.

In 1995 the colonial government of Hong Kong enacted the *Personal Data (Privacy) Ordinance* (1995), which covered both the public and private sectors. With the 'handover' to China in 1997 the Hong Kong SAR became the first region of the PRC with a data protection law. Six Data Protection Principles are broadly consistent with the OECD privacy Guidelines, but are stronger in some important respects. The main problem with the Ordinance is that there is no provision for the Privacy Commissioner or the Administrative Appeals Board (to whom his decisions can be appealed) to award any compensation or other remedies to complainants, or to penalise organisations for breaches unless they persist with them. A provision allowing Courts to award compensation is unused, probably due to the expense and publicity involved, so the Ordinance suffers from under-enforcement. As a result, chronic data spills go unpunished, and complainants go uncompensated.

Taiwan's *Computer Processed Personal Data Protection Act* was enacted in 1995, influenced by the OECD privacy Guidelines. It has limited coverage, dealing generally with the public sector but only eight specified private sector areas. There is no single oversight body, enforcement being left to the Ministries responsible for each industry sector. Evidence of the enforcement or effectiveness of the Act is lacking, but commentators are of the opinion that the Act is ineffective. The Executive Yuan (Cabinet) has been proposing measures to strengthen the Act since 2000 (including broader scope, stronger principles and strong enforcement), but to no effect as yet.

Since the 'June struggle' democratic movement of 1987 South Korea has changed from authoritarian and undemocratic regimes to a liberal democracy. By 2005 it had the highest distribution rate of Internet broadband networks in the world. These factors have contributed to a society where South Koreans are very conscious of the potential abuses of government power, and of Internet issues, and demand that governments be concerned about privacy protection. Like Australia and Japan, it first introduced a data

protection law covering its public sector with the *Public Agency Data Protection Act* of 1995, but it is an Act enforced by the Ministry responsible for government administration, and an oversight body from within government, which are not generally considered to be active or effective. In the private sector, the legislation is to some extent sub-sectoral, with separate laws governing credit and medical information, but the *Act on Promotion of Information and Communications Network Utilization and Information Protection* of 2001 (often called the 'Data Protection Act') applies most generally to entities that process personal data for profit through telecommunication networks and computers. The 2001 Act was influenced strongly by the OECD Guidelines, but was strengthened beyond that in 2004 in relation to data breaches, data exports and other matters. The Personal Information Dispute Mediation Committee (PIDMC) mediates disputes concerning statutory privacy breaches by private sector bodies and provides financial compensation which is enforceable once the mediation is accepted. The PIDMC committees award compensatory damages in almost all cases where a breach of privacy provisions is found, usually even when they award correction or other remedies. Damages typically range from US$100 to US$10,000. The contrast with Hong Kong and most other jurisdictions is stark. The Korean Information Security Agency (KISA) receives over 17,000 complaints per year, and acts as the secretariat for the PIDMC. Self-regulation has contributed little in South Korea, perhaps due to this effective enforcement. Since 2004 there have been repeated but unsuccessful attempts to fuse the public and private sector provisions into a comprehensive data protection system with an independent supervisory agency.

The **Macao SAR**'s *Personal Data Protection Act* (2006) is the most recent data protection law in Asia, and potentially one of the strongest. The Act is a very similar to Portugal's legislation in most respects (though also influenced by Hong Kong's Ordinance). As a result it is closer to the EU privacy Directive of 1995 than any other data protection legislation in Asia. Macao's position as a region of the PRC makes this doubly interesting. The Office for Personal Data Protection (OPDP) has administered the Act since 2007, and although it has very extensive powers has yet had little time in which to exercise them.

The ASEAN potential, and China

The next stage of development of data protection legislation is likely to come from a number of ASEAN member states that already have official drafts of legislation (Thailand, Philippines, Malaysia and Indonesia), or perhaps from China. ASEAN member countries have made a commitment to develop privacy legislation by 2015.

Thailand's *Official Information Act 1997* provides basic but incomplete data protection in relation to government agencies. It set up a 32-person Official Information Commission (OIC) and a secretariat which serves it. As well as being a freedom of information Act, it also limits personal data collection and its retention, limits disclosures, requires security, and provides access and correction rights. It is, in effect, an information privacy law in relation to the public sector. There are a number of Bills proposing coverage of the private sector, and a privacy Commissioner, but none have been successful, partly due to the current political turmoil.

The **Philippines** has little legislation as yet, but an EU-influenced Act with reasonably strong enforcement powers and a Commissioner is likely to emerge from the legislature in 2009. At present, the *Electronic Commerce Act* (2000) sets a general principle that businesses should give users choice in relation to privacy, confidentiality and where

appropriate, anonymity, but it and a set of government guidelines have had little effect. The Supreme Court adopted in 2008 as a rule of Court, a *Rule on the Writ of Habeas Data* which has potential to protect privacy but has not yet been used.

Current privacy protections in **Malaysia** are not significant, and Malaysian Ministers have been monotonously proposing to introduce comprehensive data protection legislation since 1998. However, a new Bill is known to have been prepared in 2009, but no one expects it will provide strong data protection even if enacted.

Indonesia's *Law on Information and Electronic Transaction* (2008) provides a very broad right to compensation for misuse of personal data by electronic media, but is too new to be of significance yet. A draft Bill has been prepared influenced by the OECD Guidelines and other international instruments but is not yet public.

Singapore is arguably the world's only developed country without privacy legislation. Its Model Data Protection Code (2002) is an industry-based self-regulatory code with no known effect. **Vietnam** is considering an APEC reference in a new law, but no privacy developments are known in the remaining ASEAN countries of **Myanmar, Cambodia, Laos** and **Brunei**.

In **China** an EU-style draft *Personal Information Protection Act* was under consideration until 2007, but no longer seems to be under active consideration. It was drafted in 2005 by Professor Zhou Hanhua, director of the Institute of Law at the Chinese Academy of Social Sciences and a team of experts commissioned by the Chinese government. China has no national civil law specifically protecting personal information, but some local governments are now enacting partial provisions. The Seventh Amendment to the Criminal Law of the PRC (February 2009) criminalises a wide range of disclosures of personal information and the obtaining of same, and is the first time that personal information has been directly protected by the criminal law in China. Any extension of information privacy rights in China will have a strong influence throughout the region.

To complete the east Asian picture, **Mongolia** has taken a unique route, adopting a Law on Personal Secrecy (1995) and Law on Personal Secrecy (Privacy Law), affecting laws covering various types of personal information and creating a right to sue for breaches, and regulate exceptions. There is training for officials, including taking of an oath.

India, outsourcing and South Asia: The recalcitrant zone

South Asia may be the 'final frontier' for data protection in Asia, but the situation there is capable of rapid change. Regional agreements are unlikely to be a factor, as SAARC has shown little interest in privacy, but commercial pressure from Europe may be.

India has no significant data protections laws in force as yet. The *Information Technology Act 2000* covers little of significance to data protection, and has not been enforced. Amendments to it in 2008 may provide remedies for disclosure of 'sensitive' information, but it depends on the regulations yet to be made. The *Credit Information Companies (Regulation) Act 2005* is a potentially significant comprehensive credit reporting code, but it is still being brought into effect by the Reserve Bank of India. The one effective aspect of data protection in India is the right of access to personal

information held by any public body in India, under the *Right to Information Act 2005*, which is actively enforced and has already generated a large body of case law. An unknown factor is whether India's Supreme Court might develop the constitutional protection of privacy in such a way that it forces the government to enact a law to provide data protection, as it did in requiring right to information legislation. There is no evidence of any effective self-regulation.

In the rest of the SAARC region (**Pakistan, Bangladesh, Sri Lanka, Nepal, Maldives, Bhutan**) there is no sign of data protection developments, other that a number of Pakistani Bills some years ago which have lapsed.

Conclusions: Slow but accelerating laws with multiple influences

From this brief snapshot of twenty one years of data protection developments, a number of themes emerge. The influences on data protection principles are principally the OECD Guidelines and the EU Directive, but the APEC Privacy Framework has not yet had any direct influence. The influence of the EU Directive is, if anything, strengthening over time. The enforcement/administration model of a central Privacy Commissioner, common in Europe and found in the first regional law (Australia) has continued to find adherents (New Zealand, Hong Kong, Macao and various Bills in Thailand, the Philippines and Korea), but the model of diffuse enforcement responsibilities is also found in North Asia (Japan, Taiwan, proposed in China) though there is little evidence of its effectiveness. Few jurisdictions have yet developed an enforcement structure that generates a significant quantity of Commissioner's case studies or Tribunal/Court decisions to ensure that the law is interpreted, New Zealand being the notable exception.

Overall, data protection laws continue to spread through Asia and the Pacific, and are accelerating if even half of the current Bills are enacted. Existing laws continue to be strengthened, and data export restrictions within the region are becoming more common (Australia, Macao, Korea, Hong Kong though not in effect, and soon New Zealand). Although the APEC processes have had little apparent influence in terms of direct adoption of principles, they may have stimulated data protection interest and legislation. Influences both external and internal to the region are likely to make data protection laws an accepted feature of legal systems across the region before PL&B has another significant anniversary.