University of New South Wales
University of New South Wales Faculty of Law Research Series
2011

Year 2011 *Paper* 30

Asia-Pacific Data Privacy: 2011, Year of Revolution?

Graham Greenleaf*

*University of New South Wales; Kyung-Hee University, g.greenleaf@unsw.edu.au

Asia-Pacific Data Privacy: 2011, Year of Revolution?

Graham Greenleaf

Abstract

Nearly a quarter of a century after data privacy laws (or as the Europeans say, 'data protection') first appeared in Asia and the Pacific, the year 2011 is developing as a watershed year. The past year to July 2011 has seen more dramatic developments in the expansion of data protection laws in Asia than any previous year. Legislative action seems to parallel the accelerating scale of threats to privacy, typified by massive data breaches in country after country, but the causal relationship is beyond the scope of this article.

This article surveys data privacy legislation developments across Asia (from Japan to Pakistan, and from Mongolia to Indonesia), plus Australasia and the Pacific. It does so by sub-regions, in order of where the most dramatic recent developments have taken place: South Asia; North Asia; Indo-China; Australasia and the Pacific. The emphasis is on developments over the last 18 months, but background on previous data privacy laws is provided.

The article also considers (i) Which factors give the best indication of the strength of privacy protection provided by laws in the Asia-Pacific?; (ii) What are the main external influences on the development of data protection in the Asia-Pacific?; and (iii) What justification is there for calling this a 'year of revolution'?

Asia-Pacific data privacy: 2011, year of revolution?

*Graham Greenleaf, Professor of Law & Information Systems, UNSW, Australia and International Scholar, Kyung-Hee University Law School, Seoul, Korea**

For publication in Kyung Hee Law Journal

31 July 2011

The accelerating growth of Asia-Pacific data privacy laws

Nearly a quarter of a century after data privacy laws (or as the Europeans say, 'data protection') first appeared in Asia and the Pacific, the year 2011 is developing as a watershed year. The past year to July 2011 has seen more dramatic developments in the expansion of data protection laws in Asia than any previous year. Legislative action seems to parallel the accelerating scale of threats to privacy, typified by massive data breaches in country after country, but the causal relationship is beyond the scope of this article.

This article starts by surveying data privacy legislation developments across Asia (from Japan to Pakistan, and from Mongolia to Indonesia), plus Australasia and the Pacific. It does so by sub-regions, in order of where the most dramatic recent developments have taken place: South Asia; North Asia; Indo-China; Australasia and the Pacific. Developments in the Americas, north and south, are a separate story not addressed here.

It then compares the legislative developments across some key criteria that indicate the strength of protection provided by each law: existence of a data protection authority (DPA); ability of individuals to obtain financial compensation; data export prohibitions; and data breach notification requirements.

Two years ago in 2009 there were seven jurisdictions in the region which had enacted data privacy laws (in chronological order of private sector coverage: New Zealand; Hong Kong; Taiwan; Australia; South Korea; Japan; Macau), and some were of limited scope (Greenleaf, 2009). Now they have been joined by India and Malaysia, but just as important is that South Korea and Taiwan have made major changes to expand and strengthen their laws. Australia and Hong Kong are in the process of so doing (just how major is still uncertain), and New Zealand has made significant changes in order to obtain an 'adequacy' rating from the EU. Even Singapore has promised a law, and China and Vietnam have introduced piecemeal protections.

* <g.greenleaf@unsw.edu.au>; Parts of this article update G Greenleaf 'Twenty-one years of Asia-Pacific data protection' (2009) *Privacy Laws & Business International Newsletter*, Issue 100, 21-24; A version of this update will also be published in *Privacy Laws & Business International Review.*

Looking at data privacy legislation only gives part of the picture of privacy protection, because constitutional rights and general provisions of civil and criminal laws may also protect privacy, but that is not addressed here.

North Asia: Change everywhere, except Japan

In North Asia almost all countries bordering the People's Republic of China (PRC) having enacted or revised data privacy laws recently, including the two Special Administrative Regions of the PRC. If China ever goes in the same direction, North Asia will become the most 'data privacy intensive' region outside Europe.

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, the *Public Agency Data Protection Act* of 1995. 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. No significant self-regulation has occurred in South Korea, perhaps due to this effective enforcement.

Since 2004 there have been repeated but unsuccessful attempts in Korea to fuse the public and private sector provisions into a comprehensive data protection system with an independent supervisory agency, and they have finally borne fruit in 2011. A new *Data Protection Act* has been passed and promulgated (March 29, 2011), and will come into force on September 30, 2011. In the intervening six months, regulations and guidelines will be made. The most important changes in the new Act (Park and Greenleaf, 2011) demonstrate the innovative nature of the Korean reforms:

(i) All data processors, public and private, are regulated by the one Act, which completely replaces the previous public sector Act. Manually processed information is now covered. Korea, Taiwan and Macau are now the civil law jurisdictions in Asia with a single comprehensive data privacy law.

(ii) An independent Data Protection Commission (DPC) under the Presidential Office, composed of 15 members (including a chairperson and a standing

commissioner) will deliberate on policy issues, laws and regulations, and investigate breaches of the Act and refer matters for prosecution. The PIDMC will now mediate both public and private sector disputes, and will come under the Commission administratively. The DPC will be the first independent national data protection authority (DPA) established in a civil law country in Asia.

(iii) Other new dispute resolution mechanisms are added. Collective mediation procedures may be used where there is widespread though minimal damages to data subjects. Representative lawsuits by consumer organisations will also be allowed, but only to seek injunctions against continuing activities infringing upon privacy subsequent to mandatory collective mediation procedures being invoked.

(iv) Collection and use of sensitive data, including universal identifiers like the resident registration number, will be prohibited without the specific consent of data subjects or authorization by law (which will have a major effect on Korean websites).

(v) Notification to data subjects of the source of personal data (other than themselves) will be required. Companies conducting marketing based on their own databases will now be required to obtain the data subjects' explicit consent.

(vi) Data subjects shall be notified of the option of refusing consent to collection or processing, and Korea's unique 'no disadvantage in case of refusal' rule is continued.

(vii) Data breach notification to the affected data subjects will be compulsory, while significant data breaches must be reported to the DPC. Data processors must take efforts to minimize the effects of breaches.

(viii) Privacy Impact Assessments (PIAs) will be required in case of potential danger to data protection in the public sector, but only encouraged in the private sector.

(ix) It extends data protection into the regulation of surveillance: CCTV may be installed in public places only for the purpose of prevention of crime.

South Korea's new law may now be the theoretical benchmark for strong data protection in Asia, but this is subject to it being tested in practice to see if it delivers what it promises.

Taiwan's *Computer Processed Personal Data Protection Act* was enacted in 1995, influenced by the OECD privacy Guidelines. It had limited coverage, dealing generally with the public sector but only eight specified private sector areas. There was 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 were of the opinion that the Act is ineffective.

Taiwan's new *Personal Data Protection Act* enacted 26 May 2010 is in effect a new piece of legislation. It will not be brought into force until late 2011 or early 2012 when the Enforcement Rules are completed. The Act is comprehensive in relation to both public and private sectors, and thus much more extensive than the previous Act in relation to the private sector. The revised Act still has no single oversight body, and does not create

a data protection authority. Enforcement is left to the Ministries responsible for each industry sector. The obligations imposed by the Act have been considerably expanded, particularly those in relation to notice, and to sensitive data. Data exports ('international transmission') by private organisations ('non-public agencies') *may* be restricted by 'the central competent authority for the relevant industry' (A 21), but this is not an automatic prohibition on exports. The Act has the first example of an enforceable requirement to notify data subjects (but not the relevant authority) of data breaches in Asian data protection legislation, but it does not apply to all 'data breaches', only to those where the company or government agency has breached a provision of the Act. Contraventions of the Act, where damage is caused to another person, can be punished by imprisonment up to two years or substantial fines. Potentially more important are the extensive provisions for damages actions, and for class action litigation (where 'the rights of multiple subjects are injured by the same causal facts') by representative organisations which have objectives of protecting personal data. While not as innovative as Korea's new law, this Act does bring Taiwan up to most aspects of international standards (Greenleaf 2010, 2011b).

In 1995 the colonial government of **Hong Kong** enacted the *Personal Data (Privacy) Ordinance* (1995), which covered both the public and private sectors, the first data protection law in Asia. 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 breaches. 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 (Greenleaf 2010a, 2010c).

In July 2011 Hong Kong's government put forward a Bill to amend the Ordinance. It does not include the extensive strengthening advocated by the Privacy Commissioner, but does propose modest improvements. Companies will always have to give individuals notice that they intend to sell their personal data, or even use it for their own marketing, but will still be allowed to do so unless the individual exercises an 'opt out' right. The Commissioner will now be able to order organisations to remedy contraventions of the Ordinance. Compensation proceedings will now be moved to a lower court, which may reduce the deterrent effect of the risk expensive court costs but will not remove them, and the Commissioner will be empowered to assist litigants. For the first time, the Commissioner will also be empowered to assist parties to reach a settlement or compromise. It is possible that the Bill may be strengthened by the legislature (LegCo), because of the extent of public disquiet over the data breach scandals involving police and hospitals, and data sales scandals involving data from the Octopus transit card, banks and telcos.

In the absence of any other useful deterrent sanctions in the current Ordinance, the Commissioner announced (June 2011) that he will 'name and shame' any organisation (company or agency) he finds has breached the Ordinance, whether or not they have discontinued the practice or made amends.

The **Macao SAR** has potentially one of the strongest data privacy laws in Asia, albeit from one of the smallest jurisdictions. The *Personal Data Protection Act* is 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 has very extensive powers (Greenleaf 2009a). It has now issued three fines for contraventions of the Act (July 2009 and May 2011), against a government agency for disproportionate disclosure when providing all of the details of a person's ID card to a mediation party who needed to locate them; against a bank for failing to observe a direct marketing opt-out; and against an individual decorating contractor for disproportionate disclosure of personal data. Perhaps more significantly, it intervened to cause the suspension of the use of mobile traffic surveillance cameras by the Traffic Services Bureau and the Public Security Police because it lacked legitimacy, in that the use might involve the collection and processing of sensitive data outside the sphere of public roads. The reasoning and the results are very European.

Japan has had an *Act on the Protection of Personal Information Held by Administrative Organs* governing public sector data since 1988. 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 (Shimpo and Greenleaf, 2011), 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. In summary, it is possible that Japan's legislation is observed by many companies and agencies, simply because it is the law, but there is no evidence at all that the law is ever enforced or that anyone ever obtains any remedies because of breaches (Greenleaf, 2010d). Japan's Consumer Affairs Agency has taken lead responsibility for the law since 2009, but it is a miniscule part of what they do; they are powerless and only seem to regard 'dissemination and awareness building' as their role; and no obvious changes have yet resulted. Japan has one of the weakest data privacy laws in Asia, and there are no signs of change.

In **China** data privacy laws have for the last five years been in what could be called the 'warring states' period, where the states in question are the many fiefdoms in the labyrinthine bureaucracies of the PRC. In 2006-7, an EU-style draft *Personal Information Protection Act* drafted at the Institute of Law at the Chinese Academy of Social Sciences was under consideration, but no longer seems to be favoured (Greenleaf 2008, 2008a). The Informatics Committee of the State Council which was considering it has been abolished. 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. The PRC *Tort Liability Law*, which came into force in July 2010 includes a right to privacy (隐私权) in its list of protected 'civil rights and interests', but without defining further what is meant. This seems to mean that data privacy violations are a tort, but case law will be needed to clarify this. Data privacy provisions have also been included in sectoral laws and guidelines in 2009/10 the fields of money laundering, medical records, insurance, consumer protection and credit reporting (Hunton & Williams, 2011). Various Provinces have also enacted local data privacy codes, particularly in consumer law. The most recent development is that in February 2011 the Ministry of Industry and Information Technology (MIIT) Standardization Administration of China (SAC) issued draft 'Guidelines for Personal Information Protection', which are only intended as a non-enforceable standard, but also contain very strict 'guidelines' concerning data exports. A State Internet Information Office parallel to the State Council Information Office has also been established, perhaps indicating an intention of tighter Internet control (May 2011). These initiatives are piecemeal and incoherent. If they are eventually replaced by a national extension of data privacy rights in China, this is likely to have a strong influence throughout North Asia and the whole region. But at present it is jurisdictions like India, South Korea and Taiwan that are setting the benchmarks while China shows no leadership, only confusion.

To complete the north 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.

South Asia: India, outsourcing, and 'adequacy'

Two years ago I described South Asia as the 'final frontier' for data protection in Asia (Greenleaf, 2009), but noted 'the situation there is capable of rapid change' if 'commercial pressure from Europe' is applied. However, unlike North Asia where data privacy developments are occurring in all countries, in South Asia India is 'going it alone'.

India sought an 'adequacy assessment' from the EU in 2009/10 (no outcome has been announced), so it is clearly desirous of a favourable view from Europe, to ease compliance burdens in relation to outsourcing. At that time it had no significant data protections laws in force. The *Information Technology Act 2000* covered little of significance to data privacy, and amendments to it in 2008 which could create remedies for disclosure of 'sensitive' information depended on Rules 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. There was no evidence of any effective self-regulation. 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. Therefore, as of 2010, the only effective aspect of data protection in India (Greenleaf, 2011a) was 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.

Six months later, the situation is quite different. India has implemented an extensive data privacy regime (limited to the private sector) through Rules made under s43A of the IT Act (as amended in 2008), which deals with negligence in providing and 'maintaining reasonable security practices' (April 2011). The essence of India's data protection scheme seems to be that the Rules made under s43A comprise part of the obligations on companies to both have in place and to implement a comprehensive information security programme (Greenleaf 2011). Whether the whole s43A scheme is *ultra vires*, or even unconstitutional, may eventually be tested by the Courts, but for now it is the law. The Rules then set out a conventional set of data protection principles with an OECD flavour. The Rules also provide data export limitations, requiring that an overseas recipient 'ensures the same level of data protection' as provided by the Rules, plus exceptions for consent and contracts. They also attempt to control what use foreign recipients make of data from India when they use it in their own countries, an innovation sure to annoy those opposed to effective data protection. Enforcement of complaints is through a special system of investigation by Adjudicating Officers, with a right of appeal to the Cyber Appellate Tribunal (CAT). There is no limitation imposed on the compensation that can be awarded under s43A by a CAT, but it cannot provide any other remedies. The whole system is as yet untested, but has the appearance of a serious data privacy regime, except for the absence of a DPA.

That absence will be remedied if a draft Bill being formulated by the government becomes a law. The draft *Privacy Bill, 2011* (India Legislative Department, 2011) will create a three person Data Protection Authority of India (DPAI). The Bill will also create a statutory right of privacy (another first for the Asia-Pacific), open-ended in its definition but including rights of confidentiality, freedom from surveillance, and protection of personal data (possibly including the specific rights under the s43A Rules system). The Bill also sets out a details data privacy code, somewhat different from that under the s43A Rules. The DPAI will have very extensive functions, including keeping a register of data controllers (a step our of keeping with all other Asia-Pacific laws), and strong powers to investigate the actions of any data controller and issue directions to them. Individuals will be able to lodge complaints against data controllers with the CAT, which would be empowered to make any orders it thinks fit including compensation. A bizarre aspect of the Bill, for a country seeking an EU adequacy finding, is that it limits its protection to Indian citizens. The Bill is very complex, including detailed controls on surveillance as well, but only a draft as yet, and will undoubtedly be modified very considerably before it progresses. But if it goes ahead in anything like this version, India may get one of the stronger Asia-Pacific privacy regimes.

In the rest of the SAARC (South Asian Area of Regional Cooperation), comprising **Pakistan, Bangladesh, Sri Lanka, Nepal, Maldives,** and **Bhutan**, there are no signs of data protection developments. Regional agreements are unlikely to be a factor, as SAARC has shown little interest in privacy. It is possible that the rapid developments in India may spark changes in its neighbours as well, both because they compete with India for outsourcing work, and because India's new law may prevent exports of personal data to them as well.

ASEAN potential, little reality (Indo-China, Indonesia and the Phillipines)

The next stage of development of data protection legislation may come from the ten member states of ASEAN (Association of South East Asian Nations), but it has not yet happened: this is still the region of nothing but promises. Malaysia is the first to enact a private sector law, but after two years it is not in force, and Singapore has announced its intention to introduce a private sector Bill in 2012. Others have official drafts of legislation (Thailand, Philippines, and Indonesia), but show little evidence of progress, and others have piecemeal legislation.

ASEAN is important because 'the ten Member Countries of ASEAN have a combined population of 575 million and a combined GDP of $US 1.8 trillion, making it one of the largest and most integrated regional organisations outside Europe', and ASEAN 'does have a history of the successful harmonisation of laws – something that is absent in APEC' (Connolly, 2008). Unlike SAARC countries, ASEAN member countries have made a commitment to develop 'best practices / guidelines' on data protection by 2015, as part of their commitment to establish an integrated ASEAN Economic Community (AEC) by 2015. Although this falls short of a commitment to legislate on data protection, it is quite possible that there will be efforts to legislate by 2015 in some of the countries.

Current privacy protections in **Malaysia** are not significant, and Malaysian Ministers monotonously proposed to introduce comprehensive data protection legislation since 1998. In 2010, they finally did so, and enacted it quickly, but there the story stops. The *Personal Data Protection Act 2010* was passed in April 2010 but is not yet in force. They have now announced they will establish a new department under the Information Communication and Culture Ministry to oversee the implementation of the Act, not to be brought into force until 2012 (Bernama.com, June 2011). It seems they are delaying as long as possible while appearing to do something. The Act will apply broadly to the business sector but not to non-business parts of the private sector, nor to government. The Personal Data Protection Commissioner required under the Act has not yet been appointed. The Commissioner hen appointed, will not meet the international Data Protection Commissioners accreditation requirements concerning independence because he or she can be dismissed by the Minister without reasons, and the Minister may also give the Commissioner general directions consistent with the Act (Greenleaf 2010f; Munir and Yassin 2010, 219-20). The seven Personal Data Protection Principles (General; Notice and Choice; Disclosure; Security; Retention; Data Integrity; and Access), and additional rights to withdraw consent for processing and otherwise prevent processing for direct marketing 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 many exceptions. 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, on the basis that the destination provides protection 'at least equivalent' to Malaysia. But it then provides far too wide a range of other exceptions by which to justify data exports, undermining the apparent restriction. The enforcement provisions in the Malaysian Act have borrowed all the serious flaws of the Hong Kong Ordinance, but worse in that there is not even the theoretical possibility of going to court to seek damages. Whereas the Japanese law is very difficult for anyone to understand, the flaws in this legislation are apparent to a casual glance.

Singapore joins the USA as the world's most developed countries without data privacy legislation. Its Model Data Protection Code (2002) is an industry-based self-regulatory code with no known effect. In February 2011 the government announced it had finally completed a study of data protection regimes and expects to introduce a data protection Bill to Parliament in early 2012. Further consultations of unstated duration are intended before enactment. 'The proposed law is intended to curb excessive and unnecessary collection of individuals' personal data by businesses, and include requirements such as obtaining the consent of individuals to disclose their personal information', are the only details revealed by the Minister. A Data Protection Council will be set up after enactment to oversee the implementation of the legislation. We can assume that, as in Malaysia, the Act will not cover the government sector, and that there will be some further years of foot-dragging before an Act is in force.

Vietnam's National Assembly passed a new *Consumer Protection Law* on November 17, 2010, which took effect on July 1, 2011, replacing the 1999 Ordinance on Protection of Consumers Rights. Its provisions strengthen consumers' rights, include those on the use, collection and transfer of consumer information, in a brief but broad data privacy code. It has been summarised as follows: 'If business entities want to collect, use and transfer information about consumers, they must satisfy the following requirements: Expressly and publicly inform consumers about the purpose of the collection and use of their information before actually collecting, using and transferring such information; Use information about consumers only for the stated purpose; Obtain consent from consumers before using their information; Ensure the secrecy, accuracy and completeness of consumer information during collection, use and transfer; Update and correct information or have a mechanism allowing consumers to update and correct information when it is discovered that such information is not accurate; and Obtain consumers' consent before transferring their information to a third party, except in cases where the law provides otherwise' (Baker & McKenzie 2010). The scope of terms such as 'personal information' and 'consent' is not defined in this law, but other laws shed some light on their meaning. The new law expands those obligations in regard to all consumers, not just in the context of e-transactions (as was the case with earlier laws), but does not change the substance of those obligations. A possible comprehensive data privacy law has been discussed at APEC meetings, but it is not clear whether one will be developed.

The **Philippines** has little legislation as yet. 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. An EU-influenced Data Privacy Bill with reasonably strong enforcement powers and a Commissioner has been before the Philippines Congress since 2009 (Parlade, 2009). The Data Privacy bill was among three non-fiscal bills filed in the 14th Congress but not passed. The Joint Foreign Chambers of commerce and the business processing outsourcing industry in the Philippines have warned that its lack of legislation on data privacy is a growing cause of concern for prospective investors and a substantial hindrance to the development of the outsourcing sector in the Philippines (Cahiles-Magkilat, 2011).

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 political turmoil in Thailand in recent years. The most recent Personal Data Protection Bill proposes a Personal Data Protection Board, and as well as a detailed data protection code includes features such as a registration system and a certification scheme (Duncan 2011).

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 (Sinta Dewi 2009), and after three years has not reached the government's legislative agenda. In contrast, the national ID Card Program was launched in 2010 and is being implemented across Indonesia by the Department of Home Affairs.

No privacy developments are known in the remaining ASEAN countries of **Myanmar, Cambodia, Laos** and **Brunei**. We await ASEAN developments by the 2015 'deadline'.

Australasia and the Pacific

Australia and New Zealand were two of the earliest countries in the region to develop data protection laws, and their law have had some influence on others in the region. In recent years weaknesses in the Australian law have become apparent, whereas the strength of the New Zealand law has been sufficient for it to (soon) receive the region's first 'adequacy' assessments from the EU.

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 case. As a result of around 200 such HRRT and Court decisions, New Zealand has a rich body of privacy law, and an Act where complainants and respondents alike can understand the consequences of breaches. In 2010 New Zealand remedied the weakest aspect of its law, the lack of a data export restriction, but (as with Taiwan) it is the softest form of restriction, requiring the Commissioner to take discretionary action to prohibit an export.

However, the improved Act, despite some other departures from EU standards, was good enough for the EU's Article 29 Working Party to consider that New Zealand's data privacy protection should be considered 'adequate' (March 2011), and a formal adequacy finding by the EU will now almost certainly follow. A contributing reason was that New Zealand is a long way from Europe, is not significantly involved in outsourced processing of the data of EU citizens, and its laws are likely to have few other effects on Europeans (Greenleaf and Bygrave 2011).

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 a series of Privacy Commissioners have been unwilling to use them. When combined with the absence of any provisions for complainants to appeal to the Courts, this has resulted in only a handful of 'determinations' by the Commissioner, and one significant Court decision, after twenty-three years. So Australia's federal privacy law is still largely unknown territory, and some agencies and companies may well treat its more difficult provisions as optional in the absence of any evidence of enforcement. 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.

The Australian Law Reform Commission commenced a review of the *Privacy Act* in 2006, and the first part of a very weak government Bill to reform it (dealing with principles) is now under consideration by Parliament, with a Senate report on the Bill suggesting few improvements (May 2011). The part of the Bill dealing with the enforcement deficiencies of the Act has not even reached Parliament after five years. However, the government has moved forward consideration of a statutory privacy action, taking advantage of the current controversies in the UK and elsewhere concerning the media and privacy (July 2011). At this stage there is little reason to expect significant improvements to Australia's performance in privacy protection. An imperfect but usable Act has been made largely redundant by lacklustre administration that has failed to create anything resembling responsive regulation.

There are no known data privacy developments in **Papua New Guinea**, **Timor Leste**, or the many countries in the **Pacific Islands**.

Factors indicating strength of laws

Which factors give the best indication of the strength of privacy protection provided by laws in the Asia-Pacific? There are dozens of factors in data privacy laws that could be used as a basis of comparison, but most are common to all laws that we would consider as data privacy laws. The factors summarised below are discriminators: factors that indicate strength or weakness of an Act, and the presence or absence of which varies considerably between Acts.

(i) *International standard principles* The initial question must be 'Do the privacy Principles meet basic international standards?' such as the Principles found in the OECD Guidelines.

(ii) *Mandatory data export restrictions* are becoming more common across the region: Australia, Macao, Korea, India, Malaysia and Hong Kong laws have them, though some are not yet in effect. Since it is not yet in force after 15 yeas, the HK restriction is not counted below. Taiwan and New Zealand have restrictions operable only at the discretion/option of their government or Commissioner.

(iii) *Limitations on marketing* Whether individuals have the ability to opt-out of direct marketing uses of their data is one indicator of the strength of an Act. An even stronger indicator is whether their information cannot be used unless they explicitly opt-in (consent) to that use of their information. Stronger again is where a jurisdiction provides a 'Do Not Call' register, whereby individuals can indicate in advance that they do not wish to obtain any direct marketing telephone calls (but not other marketing methods). This is usually by legislation separate from data privacy legislation, but needs to be considered if the other two options are to be seen in perspective.

(iv) *An independent DPA* The enforcement/administration model of a central Privacy Commissioner or Data Protection Authority (DPA), common in Europe and found in the first regional law (Australia) has continued to find adherents (New Zealand, Hong Kong, Macao, Korea, Malaysia and various Bills in Thailand, the Philippines and India), The model of diffuse enforcement responsibilities across Ministries is so far only found in North Asia (Japan, Taiwan, proposed in China) and has produced little to no evidence of its effectiveness. It is thus regarded as a weakness, and a DPA as a plus. However, if a DPA is not independent of government that is well-recongised weakness, sufficient to prevent accreditation to international associations of DPAs.

(v) *Compensation* The ability of complainants to obtain financial compensation for breaches of privacy is a litmus test of the effectiveness of any data privacy regime in delivering real remedies to individuals. However, if a compensation section in an Act has failed to produce a single result after 15 years, as in Hong Kong, and nor are there any mediated settlements of compensation, then it must be considered inoperable.

(vi) *Prosecutions* Another factor associated with effective enforcement is the availability of prosecution and criminal sanctions for breach of data privacy laws, although perhaps only in cases of repeated or serious breaches.

(vii) *Mandatory notification of 'data breaches'* (significant security breaches affecting personal data) by companies or agencies to the individuals potentially affected, and usually to a DPA as well, are one of the newest features of strong data protection regimes. At present it is only found in the new laws in Korea and Taiwan, though Ministry guidelines in Japan make this a desirable practice, and it has been recommended by Australia's law reform body.

(viii) *Transparency* A data privacy law is of little use unless those affected by it know how it is interpreted and enforced in practice, whether by the Courts or by DPAs. 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 and to communicate those interpretations to the public. New Zealand is a notable exception with numerous interpretations from Courts, Tribunals and Commissioners. The very detailed case reports in Macau, and increasingly in Hong Kong, also provide a substantial body of interpretation. No jurisdictions have adopted objective standards of reporting of mediated cases. In some jurisdictions it is too early to assess whether this will be done (N/A). 'Name and shame' The Hong Kong Commissioner is as yet the only DPA to announce that in all cases where a formal report of a complaint outcome is made, the respondent company, individual or agency will be identified, thereby adopting 'name and shame' as a deterrent tool.

Based on these (admittedly arguable) factors that distinguish between stronger and weaker data privacy laws, the as-yet-untested new Korean legislation possibly shows the most promise of strong data protection, as it will satisfy all these criteria. The Macao SAR law might also do so, but it is only for a tiny jurisdiction. Whether the Taiwan law can overcome the lack of a DPA is open to question. However, in terms of practice rather than potential, the New Zealand law, despite some deficiencies, is the benchmark law, having delivered real remedies to individuals for nearly 20 years. A more comprehensive comparison than this sketch is needed to bring out all of the significant similarities and differences between laws in the region.

EU, US, OECD and APEC: Competing influences on the Asia-Pacific?

What are the main external influences on the development of data protection in the Asia-Pacific? This brief survey has touched on the data privacy laws, and proposed laws, across 45 Asia-Pacific jurisdictions, including 15 where there have been some significant developments, and 30 where there have not, including 15 small Pacific Island jurisdictions. It suggests that the following international standards, foreign states, and international organisation have influenced the development of data privacy protection in approximately this order:

(i) The *European Union's privacy Directive* (European Union 1995) has been most influential through being seen as the 'global benchmark', and because of the desire to obtain a finding that local laws are 'adequate' by EU standards. Its influence is already seen in India; Macao; Korea; Malaysia; the Philippines; China; and recently in New Zealand. The influence of the EU Directive is, if anything, strengthening over time. This could increase as a result of the expected confirmation by the European Union that New Zealand's law is 'adequate', if other Asia-Pacific countries such as India or Korea attempt to emulate New Zealand.

(ii) The *OECD Privacy Guidelines* (OECD 1980) had an earlier, and continuing influence in Australia; New Zealand; Hong Kong; Korea; Japan; and reportedly in Indonesia. The structure and wording of its principles are sometimes more familiar to the drafting styles of common law countries than those of the EU Directive.

(iii) *The USA's influence* is significant, but difficult to assess as it does not offer any particular model to other countries to emulate, other than an approach that often values sectoral laws and self-regulation of various types. It is mainly a negative influence in opposing particular provisions in data privacy laws that are perceived to have a possible adverse effect on US business. It certainly played a role in influencing the APEC Privacy Framework to be such a weak standard.

(iv) The *APEC Privacy Framework* (APEC 2005) has not yet had any direct influence that is apparent, in terms of direct adoption of principles (other than one proposed provision concerning data export limitations in Australia). Its principles are similar to those of the OECD, though inferior in some respects) and have been described as 'OECD Lite' (Greenleaf 2003 and 2009b). The Framework says nothing about enforcement mechanisms. However, APEC does provide a regular opportunity for government representatives from many countries in the region to meet to discuss privacy issues and may continue to stimulate data protection interest and legislation in new countries – even if the model adopted is that of the EU Directive.

(v) *APPA (Asia Pacific Privacy Authorities),* originated as the meeting of Australian State and federal DPAs, but is now the regional association of DPAs. Its definition of Asia-Pacific covers the USA and Canada, and at least the west coast of central and south America (Mexico), and so is somewhat APEC-like in scope. India is not an APEC member, and if it does acquire a DPA it will be interesting to see if it is let into APPA. Like APEC, APPA has a limited influence. It does not make collective decisions on policy matters, partly because (unlike the EU's Article 29 Working Party) it does not have any mandate to do so from an international agreement. It has agreed on some useful administrative guidelines for DPAs, in areas such as standards for case reporting, and cooperation in complaint investigation. At their 35th Forum in Korea in May 2011 they agreed to explore 'mechanisms to further enhance coordination between members conducting investigations into similar matters', such as the Sony Playstation data spill. But unlike its EU cousin, it is not a driver for change and policy development.

(vi) The *Council of Europe Data Protection Convention* (Council of Europe 1981) is included in this list because, although it has not yet had any significant effect in the Asia-Pacific, it has expressly been open to accession by non-European States since 2008 with the aim of developing it into a global data protection convention. If Asia-Pacific countries with high levels of data privacy protection started to become member states of the Convention, then free flows of personal data would start to become legal requirements both between European and non-European states, and between those non-European states which are parties to the Convention. In the future, this may see the Convention being a more significant influence in the Asia-Pacific.

What constitutes a year of revolution?

From the survey in this paper we can see that the past year has delivered significant changes in many countries in the region: a startling new adoption of data privacy law in India, soon to be the world's most populous country, with promise of more to come; much stronger new laws in South Korea and Taiwan, containing new elements for regional laws; new legislation in Malaysia, and promises of such across the Straits in

Singapore; new approaches to enforcement in Hong Kong and Macao; the region's first 'adequacy' assessment a step closer in New Zealand; Bills for new Acts in Parliament in the Philippines and possibly still in Thailand; reform Bills and policies in Australia and Hong Kong; consumer protection provisions in Vietnam; and in China (last but certainly not least) new tort provisions, and somewhat confusing draft 'standards'.

A reasonable conclusion is that data privacy laws have 'come to stay' across the Asia-Pacific, and that their gradual spread to other Asian jurisdictions now appears to be inexorable. Furthermore, a weak model of data protection (such as could have been derived from the APEC Privacy Framework) is not the general pattern, with jurisdictions such as South Korea, Taiwan, Macao and India demonstrating strong and often innovative provisions. It may be that 2011 will in hindsight be recognised as a revolutionary year for data protection.

References

APEC (Asia Pacific Economic Cooperation) (2005) *APEC Privacy Framework*, available at <http://publications.apec.org/publication-detail.php?pub_id=390>

Australian Senate (2011) Report on Privacy Amendment Legislation <http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/report_part1/index.htm>

Baker & McKenzie (2010) 'Vietnam's New Consumer Protection Law Consolidates Consumer Rights on Protection of Personal Information' *Client Alert*, December 2010

Bernama.com (2011), 'New Department To Oversee Implementation Of Malaysian Personal Data Protection Act 2010', 20 June 2011 at <http://www.bernama.com.my/bernama/v5/newsgeneral.php?id=595355>

Cahiles-Magkilat, B (2011) 'Lack of legislation on data privacy protection worries investors – JFC' Manila Bulletin, June 7, 2011 at <http://www.mb.com.ph/articles/321581/lack-legislation-data-privacy-protection-worries-investors-jfc>

Connolly, C (2008) 'A new regional approach to privacy in ASEAN', Galexia website, 2008 at <http://www.galexia.com/public/research/articles/research_articles-art55.html>

Council of Europe (1981) *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series No. 108; adopted 28th Jan. 1981

D Duncan 'Personal Data Protection in Thailand' 20 July 2011, Tilleke & Gibbins website, available at <http://www.mondaq.com/x/139148/Privacy/Personal+Data+Protection+in+Thailand>

EU Directive (1995) *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data,* adopted 24th Oct. 1995 (Official Journal of the European Communities (O.J.), L 281, 23rd Nov. 1995, p. 31 *et seq.*)

Greenleaf, G (2011) 'India attempts data protection by regulations' *Privacy Laws & Business International Report*, Issue 110, April 2011

Greenleaf, G (2011a) 'The Illusion of Personal Data Protection in Indian Law' (2011) 1 (1): 47-69 *International Data Privacy Law*, Oxford University Press, available at <http://idpl.oxfordjournals.org/content/1/1/47.full>

Greenleaf, G (2011b) 'Breach notification and diffused enforcement in Taiwan's DP Act' *Privacy Laws & Business International Report*, Issue 109, 12-13, February, 2011

Greenleaf, G (2011c) 'Outsourcing and India's new privacy law: No cause for panic' *Privacy Laws & Business International Report*, Issue 111, 16-17, July, 2011

Greenleaf, G (2010) 'Taiwan revises its Data Protection Act' 108 *Privacy Laws & Business International Newsletter* 8-10 (December 2010)

Greenleaf, G (2010a) 'Octopus, insurers, banks, Commissioner, snared in Hong Kong data sales scandal ' (2010) 107 *Privacy Laws & Business International Newsletter* 8-9 (October 2010)

Greenleaf, G (2010b) 'Country Studies B.2 – AUSTRALIA' in Korff, D (Ed) Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' European Commission D-G Justice, Freedom and Security, May 2010, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B2_australia.pdf>

Greenleaf, G (2010c) 'Country Studies B.3 – HONG KONG' in Korff, D (Ed) Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' European Commission D-G Justice, Freedom and Security, May 2010, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B3_hong_kong.pdf>

Greenleaf, G (2010d) 'Country Studies B.5 – JAPAN' in Korff, D (Ed) Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments' European Commission D-G Justice, Freedom and Security, May 2010, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B5_japan.pdf>

Greenleaf, G (2010e) 'Australia's proposed reforms (Pt II): Privacy remedies' (2010) 104 *Privacy Laws & Business International Newsletter* 10-12, April 2010

Greenleaf, G (2010f) 'Limitations of Malaysia's data protection Bill' (2010) 104 *Privacy Laws & Business International Newsletter* 1, 5-7, April 2010

Greenleaf G (2010g) 'Australia's proposed reforms: Unified Privacy Principles' (2010) 103 *Privacy Laws & Business International Newsletter*, 15-17, February 2010

Greenleaf, G (2009) 'Twenty-one years of Asia-Pacific data protection' (2009) *Privacy Laws & Business International Newsletter*, Issue 100, 21-24

Greenleaf, G (2009a) 'Initial enforcement of Macao's data protection law' (2009) 101 *Privacy Laws & Business International Newsletter*, 9,27, October 2009

Greenleaf G (2009b) 'Five years of the APEC Privacy Framework: Failure or promise?' '(2009) *Computer Law & Security Report* 25 CLSR 28-43

Greenleaf, G (2008) 'Enforcement aspects of China's proposed Personal Information Protection Act' (Part II) *Privacy Laws & Business International Newsletter*, Issue 92: 11-14, April 2008

Greenleaf, G (2008a) 'China proposes Personal Information Protection Act' (Part I) *Privacy Laws & Business International Newsletter*, Issue 91: 1-6, February 2008

Greenleaf, G., *Australia's APEC privacy initiative: the pros and cons of 'OECD Lite'*, *Privacy Law & Policy Reporter*, *2003*, 10(10), p. 1–6; longer version available at <http://www2.austlii.edu.au/~graham/publications/2004/APEC_V8article.html>

Greenleaf G and Bygrave L (2011) 'Not entirely adequate but far away: Lessons from how Europe sees New Zealand data protection' *Privacy Laws & Business International Report*, Issue 111, 7-8, July, 2011

Greenleaf, G and Waters, N (2010) 'Australian Privacy Principles' – two steps backwards' (2010) 106 *Privacy Laws & Business International Newsletter* 13-15, August 2010

Hunton & Williams LLP (2011) 'A Summary of Developments in Personal Information Protection in China since August 2009', Hunton & Williams website 2011 (no longer available on web)

India, Legislative Department (2011) Draft *Privacy Bill 2011* (Third Working Draft, Legislative Department, 19 April 2011), available at <http://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf>

Munir, A and Yasin, S (2010) *Personal Data Protection in Malaysia* Sweet & Maxwell Asia, 2010

OECD Guidelines (1980) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* adopted by O.E.C.D. Council on 23rd Sept. 1980 (O.E.C.D. Doc. C(80)58/FINAL)

Park W and Greenleaf G (2011) 'Korea reforms data protection Act' *Privacy Laws & Business International Report*, Issue 109, 20, February, 2011

Parlade, C (2009) 'Philippines likely to adopt EU-style privacy and DP law' *Privacy Laws & Business International Newsletter*, Issue 95, 16-18, October , 2008

Rule J and Greenleaf G (Eds) (2008) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008

Shimpo F and Greenleaf G (2011) 'Japan's privacy complaints listed' *Privacy Laws & Business International Report*, Issue 109, 9-10, 16, February, 2011

Sinta Dewi, (2009) 'Indonesia's plans for privacy law' *Privacy Laws & Business International Newsletter*, Issue 97, 17, February, 2009

Yeo, V (2011) 'S'pore sets data protection law for 2012', 16/2/2011 on ZNet website at <http://www.zdnetasia.com/spore-sets-data-protection-law-for-2012-62206733.htm>