University of New South Wales Law Research Series

BANKERS' DUTIES AND DATA PRIVACY PRINCIPLES: GLOBAL TRENDS, AND ASIA-PACIFIC COMPARISONS

GRAHAM GREENLEAF AND ALAN L TYREE

In Sandra Booysen & Dora Neo (Eds), *Can Banks Still Keep a Secret? Bank Secrecy in Financial Centres Around the World* (Cambridge, 2017) 31
[2017] *UNSWLRS* 28

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

Bankers' duties and data privacy principles: Global trends, and Asia-Pacific comparisons

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia
Dr Alan Tyree, formerly Landerer Professor of Information Technology Law, University of Sydney
December 2015

Published as:[*] Graham Greenleaf and Alan Tyree 'Bankers' duties and data privacy principles: global trends, and Asia-Pacific comparisons' in Sandra Booysen & Dora Neo (Eds), *Can Banks Still Keep a Secret? Bank Secrecy in Financial Centres Around the World*, Cambridge, 2017, pp. 31-61, ISBN: 9781107145146.[**]

This is a pre-publication draft. Please cite the published version.

Contents

[*] This chapter was first presented at the Banking Secrecy Symposium, 4-5 December 2014, Centre for Banking and Finance Law, National University of Singapore.

[**] See <http://www.cambridge.org/gb/academic/subjects/law/financial-law/can-banks-still-keep-secret-bank-secrecy-financial-centres-around-world?format=HB#yVvLXkvPZ8hCl9FA.97>

Introduction – The uncomfortable obligations of modern banking

An examination of the relationship between the traditional duties of banks to their customers and data privacy laws is of increasing international relevance because of the growing ubiquity of data privacy laws. As is explained in other chapters,[1] at the end of the 1980s the Vienna Convention required state parties to criminalise money laundering, and the Financial Action Task Force (FATF) started development of its '40 recommendations' including 'suspicion-based reporting' to a state authority, exemption of banks from any consequent breaches of bank-customer confidentiality, and similar exemption of international requests for mutual assistance. The enactment by legislatures across the world of those recommendations, and subsequent recommendations concerning measures for reporting of 'suspicious transactions', counter-terrorist financing, anti-sanctions avoidance, and anti-corruption, have led to the global retreat of the banker's traditional duty of confidentiality in an increasingly wide and complex range of circumstances, beyond the acronym 'AML-CTF'.[2]

However, since the 1970s a somewhat inconsistent development to which banks (among other entities) were subject gradually became 'globalised': the development of 'data privacy' laws (also called 'data protection' and 'information privacy' laws), which imposed on banks an overlapping but very different range of obligations from the traditional duties owed by banks to their customers.

This chapter first explains both the contours of the increasingly global phenomenon of data privacy laws, and that these laws have considerable uniformity in their content. The core principles of data privacy laws are then examined, using examples from jurisdictions in the Asia-Pacific,[3] comparing those principles with the duties of bankers. Conclusions are drawn about the extent to which the two differ or are similar, and the overall approach that banks might take to dealing with the diversity of data privacy laws.

Banks everywhere will increasingly have to take into account data privacy laws, in addition to their traditional duties. The breadth of obligations imposed by these laws, while often in parallel with traditional duties, are generally of much broader scope, and will require new accommodations in banking practice, particularly for banks with multinational operations. However, the statutory exceptions to data privacy laws, particularly in relation to law enforcement and revenue protection, will very often apply to banks, and the specific statutory provisions concerning AML-CTF will usually override the requirements of data privacy laws. The standards imposed by data privacy laws, and penalties for their breach,[4] are becoming stronger, and that is likely to continue to occur.

The international trajectory of data privacy legislation

Over forty years ago, Sweden's *Data Act 1973* was the first comprehensive national data privacy law, and the first such national law to implement what we can now recognise as a

[1] See in particular the chapters in this book by Dora Neo, Chizu Nakajima and Stephen Pau.

[2] Anti-money laundering-counter terrorism financing.

[3] Parts of this chapter are based on Chapter 3 parts 3.1 and 3.2 and Chapter 17 of G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, 2014).

[4] There is no scope in this chapter to demonstrate the rising enforcement standards, see Greenleaf *Asian Data Privacy Laws*, chapter 18.

basic set of data privacy principles.[5] As of December 2015 there were 109 such laws, an average rate of increase of 2.6 additional countries per year for the last 42 years.[6] The picture that emerges from analysis of the growth of these laws over time is that data privacy laws are spreading globally, and their number and geographical diversity accelerating since 2000. Before further analysing this global growth, it is necessary to clarify what is meant by a 'data privacy law'.

The minimum standard for a 'data privacy law'

The privacy principles in the two earliest international instruments on data privacy, the OECD privacy Guidelines of 1980[7] (the OECD Guidelines) and the Council of Europe (CoE) data protection Convention 108 of 1981,[8] (Convention 108) can be summarised as the following ten principles (the minimum principles):

1. *Data quality* – relevant, accurate, & up-to-date
2. *Collection* - limited, lawful & fair; with consent or knowledge
3. *Purpose specification* at time of collection
4. *Notice* of purpose and rights at time of collection (implied)
5. *Uses & disclosures limited* to purposes specified or compatible
6. *Security* through reasonable safeguards
7. *Openness* re personal data practices
8. *Access* – individual right of access
9. *Correction* – individual right of correction
10. *Accountable* – data controller with task of compliance

In a series of analyses since 2011 and accompanying Tables of data privacy laws,[9] Greenleaf has charted which countries have data privacy laws.[10] The assumption on which the analysis is based is that a data privacy law must include as a minimum (i) access and correction rights ('individual participation'), (ii) some 'finality' principles (limits on use and disclosure based on the purpose of collection), (iii) some security protections; and (iv) overall, at least 8 of the 10 principles identified above (ie at least five others).[11] These comprise a basic or minimum set of data privacy principles with some pedigree in international agreements and academic scholarship.[12] The minimum standard for a data privacy law also requires some methods of

---

[5] In 1970 both the USA's *Fair Credit Reporting Act* and a data protection law for public sector in the Lander of Hessen, Germany, had included sets of data protection principles, but did not have the scope required for laws considered here.

[6] Greenleaf, G 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (on SSRN at http://ssrn.com/abstract=2280877), (2014) 23(1) *Journal of Law, Information & Science* Special Edition 23(1) Privacy in the Social Networking World, from which part of this section is derived.

[7] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, Paris, 1981); adopted as a Recommendation of the Council of the OECD, 23 September 1980.

[8] *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, opened for signature 28 January 1981, CETS No 108 (in force 1 October 1985).

[9] This analysis is presented in greatest detail in Greenleaf, G 'Sheherezade and the 101 data privacy laws'.

[10] For this purpose, a country (including any independent legal jurisdiction) is considered to have a 'data privacy law' if it has one or more laws covering the most important parts of its private sector, or its national public sector, or both.

[11] The published analyses take a slightly more complex approach, breaking the 10 listed principles into 15, and requiring 11 of the 15 overall, but this equates approximately to 8 of the 10 listed here.

[12] Principles concerning minimal collection, retention limits and sensitive information are not included, as they only became common requirements in the 'second generation' of data privacy laws and agreements from the 1990s onwards (as discussed below).

officially-backed enforcement (ie not only self-regulation). The most recent analysis (February 2015) showed that the number of countries with such laws had expanded by 10 to 109 since mid-2013.[13]

Patterns of global growth of data privacy laws

The global rate of expansion of countries with data privacy laws has averaged approximately 2.6 laws per year for 42 years. Viewed by decade, growth has been: 9 (1970s), +12 (1980s), +20 (1990s), +39 (2000s) and +29 (5.2 years of the 2010s), giving the total of 109. Such laws are now found in all geographical regions except the Pacific Islands.[14] In 2015, for the first time, the majority of data privacy laws are found outside Europe (56 to 53). European laws will increasingly be in the minority, as there is almost no room for their expansion within Europe, since it now has near-full adoption.[15] Growth is likely to continue, with at least 21 more countries currently having official Bills working their way through political and legislative processes.[16] Other new developments such as the African Union's 2014 Convention on cybercrime, e-commerce and data protection,[17] are likely to promote further growth. On current projections, by 2020 there are likely to be at least 140 countries with such laws,[18] including most of the world's economically significant countries. Countries without comprehensive private sector laws may well have significant e-commerce or consumer sector privacy laws with similar effects on the banking sector, as do China, Indonesia, Turkey and the USA at present. Laws which have a strong 'family resemblance' to at least the minimum data privacy principles listed above will be close to ubiquitous by the end of the decade. This ubiquity will require changes to banking practices.

'European' data privacy standards, and beyond

The 'minimum' data privacy principles of the early 1980s, discussed above, are no longer the prevailing international standard, including outside Europe. From the early 1990s an extended set of principles were developed for the EU data protection Directive adopted in 1995,[19] but they were based on, and incorporated the 1980s minimum principles described above.[20] The following list[21] of the most significant differences in relation to privacy principles

---

[13] Greenleaf, G 'Global data privacy laws 2015: 109 countries, with European laws now in a minority' (2015) 133 *Privacy Laws & Business International Report,* 14-17 <http://ssrn.com/abstract=2603529>. The additional ten countries are: South Africa, Kazakhstan, Mali, Ivory Coast, Lesotho, Brazil and the Dominican Republic, plus three small former Dutch colonies (Curaçao, the BES Islands and St Maartens).

[14] EU (28); Other European (25); (sub-Saharan) Africa (17); Asia (12); Latin America (10); Caribbean (7); Middle East (4); North America (2); Australasia (2); Central Asia (2); Pacific Islands (0).

[15] The exceptions are Belarus (less likely) and Turkey (more likely).

[16] See the annexed *Global Table of Data Privacy Bills* in Greenleaf 'Global data privacy laws 2015', which lists known official Bills for new Acts, both those which have been introduced into legislatures, and those which are under official consideration by governments. Information is included about the current known state of a Bill.

[17] Greenleaf, G and Georges, M "The African Union's data privacy Convention: A major step toward global consistency?" (2014) 131 *Privacy Laws & Business International Report,* 18-21.

[18] If the current rate of expansion for 2010-2015 continues in a linear fashion, over 50 new laws would result in this decade, bringing the total to 140. However, the growth of data privacy laws since the 1970s has been one of continued acceleration, not linear growth, which if it continues would result in between 140 and 160 (ie 60 to 80 new laws this decade).

[19] European Communities (EU) *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.*).

[20] They also included some additional elements already found in the CoE Convention, which was itself 'updated' in 2001 via its Additional Protocol, to reflect principles from the EU Directive. See Council of Europe, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory*

between these 'European' instruments and the minimum 1980s instruments is not comprehensive[22] but is sufficient to demonstrate the higher, stricter standards the former require. There are eight 'European' content principles[23] that may be found in national privacy laws, called in summary[24]: *(i) Data export restrictions based on destination; (ii) Minimal collection; (iii) 'Fair and lawful processing'; (iv) 'Prior checking' of some systems; (v) Deletion; (vi) Sensitive data protections; (vii) Automated processing controls; and (viii) Direct marketing opt-out.* None of the aforegoing eight elements is required, or even recommended, by the OECD Guidelines.[25]

It is a common but mistaken assumption that only the minimum standard of data protection is achieved by the laws of most countries outside Europe.[26] An analysis was undertaken of the laws of 33/39 countries outside Europe[27] with data protection laws as at December 2010 [28] It showed that in relation to 10 principles that were more strict than the OECD/CoE minimum principles (the above eight, plus two concerning enforcement), the 33 non-European laws examined on average included 7/10 of the abovementioned 'European' principles. Some of these additional 'European' principles occurred in more than 75 per cent of the 33 countries assessed, including (i), (ii), (v) and (vi) above.

No post-2010 global comparison has yet been done. However, further analysis in 2014 of eleven Asian countries with data privacy laws (including China for this purpose) showed that, on average, each of the eight 'European' principles described above is implemented in five of the eleven Asian jurisdictions, and on average each jurisdiction implements almost four of these principles.[29] These Asian jurisdictions could therefore, on average, be described as 'halfway' between the minimum principles and the 'European' principles. This generalisation probably holds true for most other regions outside Europe.

The strengthening of data protection laws is far from complete. The EU is in the final stages of reform of the data protection Directive, almost certainly by replacing it with a Regulation (the 'General Data Protection Regulation, GDPR), and has finalised this in 2016. The EU is likely to strengthen most of its standards, but nothing can be considered final until all negotiations are

---

authorities and transborder data flows, Strasbourg, 8.XI.2001, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm>.

[21] This was first argued in Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2(2) *International Data Privacy Law*, pp. 68–92 <http://papers.ssrn.com/abstract_id=1960299>.

[22] Other 'European' elements could be added to the list, for example the right to prevent further processing, but it was decided to keep the list to a manageable size. A choice was then made of the most important distinguishing elements.

[23] The original analysis also included two 'European' enforcement requirements ((ix) requirements of a DPA, and (x) access to court remedies), and so was put in terms of how many out of 10 principles (not 8) a law embodied.

[24] For more details see Greenleaf Asian Data Privacy Laws, p56; alternatively Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe'.

[25] Nor are they required or recommended by the APEC Privacy Framework (2004), which is based substantially on the OECD Guidelines of 1980.

[26] Laws in European countries can be assumed to exhibit generally higher standards, because of the requirements of the EU Directive, and the Additional Protocol to the CoE Convention.

[27] Copies, or translations, of six of the 39 laws were not available, so only 33 were examined.

[28] Greenleaf, G, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2(2) *International Data Privacy Law* at <http://papers.ssrn.com/abstract_id=1960299>.

[29] Greenleaf, G *Asian Data Privacy Laws*, pgs. 502-3.

complete. At least 15 new elements have been identified as possible components of such enhanced principles,[30] but those finally adopted may differ considerably. The enforcement provisions after reform of the Directive may also set a much stronger standard.

Implications of ubiquitous 'European' privacy standards for banks

If something close to the content of the GDPR drafts under discussion is enacted, this will constitute, in conjunction with an ongoing 'modernization' of CoE Convention 108,[31] a 'third generation' of data privacy principles, again of primarily European origins. Like the '2nd generation' European principles, they can be expected to gradually but strongly influence the shape of non-European data privacy laws.

Whether we are talking about the near-future of global privacy laws embodying something close to '2nd generation' European standards, or in future embodying '3rd generation' standards, the global reality for banks will be a world that requires compliance with something resembling European privacy laws. It will therefore be prudent and practical for banks with multinational operations, if they wish to have consistent privacy practices across countries of operation, to consider adopting a set of privacy standards which are considerably higher than the 1980s minimum principles , and which adopt the most significant and widely enacted 'European' standards. They will then have to adjust these data privacy obligations according to their local AML-CTF etc obligations.

Principles in data privacy laws, compared with bankers' duties

The principal obligation of a bank which is relevant for comparison with data privacy laws is the bank's duty of secrecy which, in common law countries, received its classic exposition in *Tournier v National Provincial & Union Bank of England* as an implied term in the contract between bank and customer.[32] There are also statutory sources of the obligations of bank secrecy, as in Singapore[33] and Switzerland,[34] but these appear to have a less consistent conceptual basis across jurisdictions.[35] The contractual duty as described in *Tournier* is therefore used as the main point of comparison in this chapter, although this does result in a necessary over-simplification.

The most important thing about data privacy laws, compared with the specific legal rules concerning bank secrecy (whether from statutory banking laws or at common law) is the

---

[30] These may include more explicit consent (opt-in) requirements, and obligations to prove same; more explicit requirements of data minimization at collection; a 'right to be forgotten'; a right to data portability, including a right to obtain a copy of personal data in a portable format; regulation of automated 'profiling'; demonstrable implementation of privacy principles (stronger 'accountability'); implementation 'by design'; implementation 'by default'; liability of local European representatives of a processor; mandatory data breach notification; the ability to require privacy impact assessments; data protection officers required; more specific requirements in relation to data exports; EU rules to apply to extraterritorial offering of goods, services, or monitoring; and a right to online subject access. This summary is derived substantially from an early analysis in February 2012, Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) *Bloomberg BNA Privacy and Security Law Report*, 6 February 2012, pp. 1–15, <http://ssrn.com/abstract=2162781>. Some elements will probably be dropped in the final Regulation.

[31] Greenleaf, G 'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty? ' (2013) *Computer Law & Security Review*, Vol 29, Issue 4 <http://ssrn.com/abstract=2262296>.

[32] [1924] 1 KB 461. See A Tyree *Banking Law in Australia*, 8th Ed, LexisNexis, 2014.

[33] See Booysen chapter in this book.

[34] See Nobel chapter in this book.

[35] D Neo 'A conceptual overview of bank secrecy', chapter in this book.

much wider range of obligations that they impose on banks concerning personal data, and that they are not limited to customer data. They encompass, as well as disclosure restrictions (where comparisons with bank secrecy laws may be readily drawn), collection limitations, limits on internal use by banks, limits on overseas transfers, obligations concerning access and correction, data quality and security. Some of these obligations may also arise from banking statutes.

To explain this wider range of obligations, this section summarises and compares the data privacy laws in Asia[36] plus in some cases, Australia but not other Asia-Pacific countries with data privacy laws.[37] It assesses how far beyond the requirements of banking law these privacy obligations extend, and to what extent these laws are similar and consistent, once we go beneath the generalisation that all are in the family of 'data privacy laws'. The exceptions to these principles which are of particular relevance to banks are often not detailed here, because they vary so much between jurisdictions.

We will focus on the following comparisons between data privacy laws and bank's secrecy duties:

1. 'Personal data' vs 'customers data', and other differences in scope
2. Minimum collection vs 'know your customer'
3. Use and disclosure restrictions vs *Tournier* exceptions
4. International dimensions of banking disclosures
5. Security & data breach vs safe custody duties
6. Access, correction and other new customer rights

Data privacy laws in Asia and Australia, and complaints concerning banks

Twelve Asian jurisdictions have significant data privacy laws affecting their private sectors.[38] Six of these laws are comprehensive, covering both the public and private sectors: Hong Kong,[39] Japan,[40] South Korea,[41] Macau,[42] the Philippines[43] (not yet in force), and Taiwan.[44]

---

[36] This comparison is derived in part from Chapter 17 of G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014). For the details of the laws of each jurisdiction, see the relevant country chapters in Part II of that book. For the sake of readability of these comparisons, legislative citations are not given. They may be found in the relevant chapters of the book. The relevant legislation is listed below.

[37] New Zealand, Canada, the United States, Mexico and various South American countries.

[38] This paper does not consider Nepal and Thailand, the laws of which cover their public sectors only. A Bill dealing with the private sector was before the previous Thai legislature in 2013: See Greenleaf Asian Data Privacy Laws, Ch. 12.

[39] Personal Data (Privacy) Ordinance 1995 (Hong Kong SAR); see Greenleaf *Asian Data Privacy Laws*, Ch. 4.

[40] Act on the Protection of Personal Information 2003 (Japan) and related legislation; see Greenleaf *Asian Data Privacy Laws*, Ch. 8. The Japanese law has now been reformed comprehensively, but the reforms are not yet in force: see Greenleaf, G 'Japan: Toward international standards – except for 'big data' (2015) 135 *Privacy Laws & Business International Report,* 12-14 <http://ssrn.com/abstract=2649556>.

[41] Personal Information Protection Act 2011 (South Korea); see Greenleaf *Asian Data Privacy Laws*, Ch. 5.

[42] Personal Data Protection Act 2005 (Macau SAR); ; see Greenleaf *Asian Data Privacy Laws*, Ch. 9.

[43] Data Privacy Act 2012 (Philippines); see Greenleaf *Asian Data Privacy Laws*, Ch. 12.

[44] Personal Data Protection Act 2010 (Taiwan) ; see Greenleaf *Asian Data Privacy Laws*, Ch. 6.

Three others cover most of the private sector (India,[45] Malaysia,[46] and Singapore[47]), and a further three (China,[48] Vietnam,[49] and Indonesia[50]) have data privacy laws which cover their e-commerce and consumer sectors. Any of these countries may also have data privacy laws specific to the banking sector[51] or other related financial sectors (eg credit reporting),[52] which go beyond being only bank secrecy rules, and include the other minimum elements of a data privacy law.

There are few examples of court actions being taken to enforce data privacy principles against banks. There are examples in the available data, of complaints of breaches of these principles by banks reported by the data protection authorities (DPAs) or Privacy Commissioners in the databases of the International Privacy Law Library.[53] From Asian jurisdictions, significant numbers of complaint examples are only available from Hong Kong SAR, Macau SAR and South Korea (though generally only in Korean).[54] However, significant numbers of complaint examples are available from Australia, New Zealand, Canada, and the (US) FTC's jurisdiction.

Differences in scope: 'Personal data' vs 'customers' data'

Data privacy laws have generally wider scope than banking laws. Banks do not usually have general exemptions from data privacy laws, but statutory requirements may in effect exempt them from particular data privacy principles in some situations.

Banks are generally not exempt

Where data privacy laws do exist and cover the private sector, it is very unusual to find any wholesale exemptions for the banking or financial sector *per se*, and none are found in Asian data privacy laws at present. Banks are therefore 'data controllers' (or similar terms) in relation to all persons whose personal data they hold or otherwise control, not only their customers. The application of the laws to persons, data and transactions may differ somewhat between countries.

---

[45] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India); see Greenleaf *Asian Data Privacy Laws*, Ch. 15.

[46] Personal Data Protection Act 2010 (Malaysia); see Greenleaf *Asian Data Privacy Laws*, Ch. 11.

[47] Personal Data Protection Act 2012 (Singapore); see Greenleaf *Asian Data Privacy Laws*, Ch. 10. See also Greenleaf, G 'Regulations bring Singapore's data privacy law into force' (2014) 130 *Privacy Laws & Business International Report,* 1-4.

[48] SC-NPC Decision on Internet Information Protection 2012 (China), SC_NPC Amendments to the Consumer Law 2013 (China), and subsidiary legislation; see Greenleaf *Asian Data Privacy Laws*, Ch. 7.

[49] Law on Information Technology 2006 (Vietnam); see Greenleaf *Asian Data Privacy Laws*, Ch. 13.

[50] Regulation on the Operation of Electronic Systems and Transactions 2012 (Indonesia); see Greenleaf *Asian Data Privacy Laws*, Ch. 13.

[51] For example, Indonesia has various provisions on privacy in its banking laws, but no general data privacy law: see DLA Piper's Data Protection Laws of the World, March 2013 <http://www.edrm.net/resources/data-privacy-protection/data-protection-laws/indonesia>

[52] This paper does not cover the requirements of specific data privacy laws relating to credit reporting, though their implications for banks are substantial, or banking-sector-specific laws. In Malaysia credit reporting practices are largely exempt from its general data privacy law.

[53] International Privacy Law Library < http://www.worldlii.org/int/special/privacy/>. It is located on the World Legal Information Institute (WorldLII).

[54] No complaint examples are yet available from the newly-established DPAs in Singapore or Malaysia, or the yet-to-be-established DPA in the Philippines. Because the laws of Japan, Taiwan, China, Vietnam and Indonesia do not establish any central DPA, examples are more difficult to find from those jurisdictions.

However, powers to create banking exemptions sometimes exist, even though not yet used. Singapore allows the Minister of Communications and Information to completely exclude any class of organization or class of data. Singapore's DPA can do likewise, with ministerial approval, granting complete or partial exemptions. Singapore's Act is also subordinate to any other Act, or any other legal requirements, to the extent of any inconsistency. In Malaysia, there is a similar ministerial capacity to exempt, on the advice of the Commission, and such exemptions may be partial or complete. Such blanket powers to create exemptions are foreign to EU law, which specifies the permissible grounds of exemption,[55] and are not found in other Asian jurisdictions.

Any blanket exemptions in data privacy laws for government access to banking records, including for security agencies, may cause problems for countries outside Europe that wish to have their data protection laws regarded as 'adequate' by the EU.[56] Even when such access is supported by specific legislation, the decision by the European Court of Justice in *Schrems*[57] underlines that they must be proportionate to the objectives to be achieved. Although the lack of 'adequacy' findings in relation to Asian countries has not yet caused major problems for their companies, but may have increased the costs of transfers from EU countries, the Schrems decision shows that major problems may arise in future.[58]

Persons protected: 'Customers' and 'personal data'

In most jurisdictions, only natural persons have data privacy rights. In Asia and Australia, legal entities are never protected by data privacy laws, only natural persons. In most cases they must also be living persons.[59] In contrast, a bank's duties are to the 'customer' in banking law, irrespective of whether the customer is a natural or legal person. In this respect, the bank's duty of secrecy is normally broader than data privacy rights.

However, the requirement that a bank is acting in its role as a bank imposes limitation on the scope of the banks' duties, although *Tournier* may extend to non-bank financial institutions, and has been held to apply to merchant banks and credit unions.[60] *Tournier* was an action for breach of contract. The New South Wales Court of Appeal has held that it only applies to the banker customer contract.[61] The result is very unsatisfactory. In *Brighton*, four guarantors were claiming a right of confidentiality. Two were customers of the bank, two were not. The two bank customers were held to have the benefit of *Tournier* in spite of the fact that their status as customers was wholly incidental to their status as guarantors. The application of

[55] EU Directive, art. 13.

[56] To put it simply, an 'adequacy' finding concerning country X by the European Commission, made under Article 25 of the data protection Directive of 1995, allows businesses in EU member states to export personal data to country X without taking any protective measures specific to the transaction (eg Standard Contractual Clauses). Such additional protective measures are often considered onerous.

[57] *Schrems v. Data Protection Commissioner* (6 October 2015) Court of Justice of the European Union (Case C-362/14).

[58] The *Schrems* decision invalidated the 'Safe Harbor' agreement between the USA and the European Union which allowed 'blanket' transfers of person data from the EU to US companies participating in the 'Safe Harbor' scheme. It is unresolved at the time of writing how future EU-US personal data transfers will take place.

[59] The Philippines and Singapore are unusual in providing that the estate of a deceased person may exercise some rights both after a person's death.

[60] For examples, see Tyree *Banking Law in Australia*, 6.2.1.

61 *Brighton* v *Australia and New Zealand Banking Group Ltd* [2011] NSWCA 152; see Tyree, "Tournier unbound" (2015) 26 JBFLP 207 for a criticism of this decision.

Tournier was extended dramatically in an English High Court case.[62] The relationship between the parties was client and sex worker. The client sought to restrain the sex worker from divulging certain information. The Court held that *Tournier* applied and that the disclosure was justified under the 'self interest' exception to the duty of confidentiality. This decision would extend the *Tournier* principles to contracts between the bank and other parties who are not necessarily customers.

However, where a bank holds a person's personal data, both 'bank' and 'customer' status are irrelevant to data privacy law. All Asian data privacy laws take the approach, conventional since the minimum principles of the 1980s and adopted in European laws,[63] that what is personal data is determined by its capacity to identify a person (not actual identification).[64] Whether the conventional definition is now sufficient for privacy protection is very questionable, but that is not the purpose of this discussion. Data privacy laws are therefore broader in the extent of the persons to whom they may apply than the *Tournier* duty of secrecy, irrespective of how broad an interpretation of *Tournier's* application is taken.

Data types protected

The bank's duty of secrecy applies at least in respect of transactions that go through the customer's account, and in relation to any securities taken by the banker, although several members of the court in *Tournier* suggested that the duty extended to any information arising out of the banking relations of the bank and its customer.

There is no *Tournier* requirement that the information must be recorded in some way. In this respect, the bank's duty of secrecy is normally broader than data privacy rights, because in data privacy laws, (in all jurisdictions except the Philippines), information must be embodied in a document before it is regulated. 'Document' is given a very wide definition, sometimes on the basis of capacity to reproduce the data (Hong Kong), or its inclusion in a database or otherwise being systematically organized (Japan, Malaysia). Information held only in a person's mind is therefore exempt, with the exception of the Philippines, which specifies that it refers to personal information 'whether recorded in a material form or not'. No Asian laws are restricted to data processed by automated means, except that of India. Other Acts include organized manual filing systems, as in Europe.[65]

'Sensitive data' principles

The European-influenced principles of additional protection for 'sensitive' personal data are found in about half of the Asian laws, notably South Korea, Macau, Malaysia, the Philippines, and Taiwan. Singapore, Hong Kong, India, Vietnam, and China do not have special protections for sensitive data. The definitions of 'sensitive data' vary considerably across jurisdictions, everywhere, but do not usually include financial data (except in India). Although the EU Directive has specified categories[66] of sensitive data, EU 'Member States differ substantially in their definitions of sensitive data, and in the permissible grounds for processing them',[67] and

62 *AVB* v *TDD* [2014] EWHC 1442 (QB); see also *Jackson v Royal Bank Of Scotland* [2005] UKHL 3 where a duty of confidentiality was implied into a transferable letter of credit transaction.

63 Kuner, *European Data Protection Law*, pp. 91–8.

64 India is the only exception to the conventional approach, because many of its principles only apply to 'sensitive' data, which is very narrowly defined but does include financial information. The application of India's law to banks is complex.

65 Kuner, *European Data Protection Law*, p. 99.

66 EU Directive, art. 8 protects 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life'; see Kuner, *European Data Protection Law*, pp. 101–3.

67 Kuner, *European Data Protection Law*, pp. 103–6 provides many examples.

do not include financial information. The Philippines has the broadest categories that could affect banks, as it adds to the EU categories marital status, age, 'education' and genetic information, and (in effect) legally privileged information. Malaysia's categories would be of limited application to banks. Banks and other businesses dealing with personal information across a range of Asian jurisdictions will need to be aware of these differences in the meaning, and administration, of sensitive personal information to avoid potential problems.

Aside from these general data protection laws, most jurisdictions are likely to have specific laws dealing with particular categories of sensitive information, particularly financial and credit information, and medical information. Japan has various separate laws dealing with such data, and a number of ministry guidelines. Hong Kong also has specific laws dealing with such matters as old criminal records, and Singapore has a number of laws dealing with 'sensitive' categories. Such sectoral laws are not covered here.

Minimum collection vs 'know your customer'

All Asian jurisdictions under consideration impose some data collection limitations based on the purpose of collection, but the majority go further and allow only minimal or necessary collection.

Minimal collection

The majority of jurisdictions in Asia (China, Hong Kong, India, South Korea, Macau, Taiwan, and Singapore) implement the stricter European approach of 'minimal' collection, that personal data should only be collected where it is necessary for a (legitimate) specified purpose,[68] rather than the weaker minimum (OECD and APEC) limitation that collection should be 'not excessive'. Japan, Malaysia, the Philippines, and Vietnam (only by implication) adopt the less strict 'not excessive' approach. Only South Korea takes the further step in data minimization, requiring that, wherever possible, transactions should be anonymous.[69] It also requires the business to prove that it only collected the minimum necessary information.

In contrast, traditional bankers' duties do not require any such minimisation of data collection. To the contrary, it is a standard element of AML–CTF legislation for banks to be required to accurately identify customers ('know your customer' – KYC). As a result, these statutory obligations will usually prevail over those in data privacy laws, whether of the 'not excessive' or 'minimal' varieties, at least to the extent specified by the relevant AML-CTF law. However, excessive collection beyond what is justified by these laws could still in theory be in breach of data privacy laws.

South Korea's data privacy law also has a very unusual explicit 'no denial of service' principle that goods and services cannot be refused because a person refuses to provide more than the minimum necessary information. Singapore is similar in the provision prohibiting organizations, as a condition of providing a product or service, from requiring an individual to consent to the collection, use, or disclosure of their personal data beyond what is reasonable to provide the product or service. These provisions give strong support to minimal collection requirements, and are not yet found in the European principles. At best, such restrictions are only implied in other laws. There are no equivalents in banking laws, and these provisions could easily conflict with 'know your customer' requirements in other laws.

---

[68] Kuner, *European Data Protection Law*, pp. 73–4.

[69] The 'anonymity principle' is rare in data privacy laws, having originated in German legislation, and also found in Australia's private sector law since 2001, but now weakened by 2012 reforms. See Kuner, *European Data Protection Law*, p. 74 concerning the German law.

Purpose of collection and notice required

The minimum principles only require that the purposes must be 'specified' by the time of collection but are ambiguous about what notice is required to the person who is the subject of the data (the 'data subject'). The European principles require that notice of such purposes must be given to the data subject,[70] as do the APEC principles. All Asian jurisdictions require that the purpose of collection be specified by the time of collection from the data subject, but in the Philippines it may be specified as soon as possible thereafter (as allowed by the minimum principles). All jurisdictions except the Philippines and Japan require notice of such purpose, and other matters, to be given to the data subject by the time of collection of personal data from the data subject. In Japan the requirement of individual notice can be avoided by a public announcement of a purpose of collection.

The content of the notice that must be given to data subjects is specified in greatly differing detail.[71] At the very specific end are China's Guidelines (but not its laws). For example, Macau requires data subjects to be informed (unless they already have the information) of the purposes of processing, the recipients of the data, the consequences of not providing the information, and rights of access and correction. Hong Kong requires much the same.

When personal data is collected from third parties (ie not from the data subject), there is a requirement to provide notice to the data subject in three laws only (South Korea, Macau, and Taiwan). This is not required in the minimum principles. Macau requires the notice to be given when the data is recorded, or not later than when it is used or disclosed. No law explicitly requires notice to be given when data is collected by observation or from documentary sources, but where laws require consent of the data subject as a condition for processing to be legal, this may have the same effect. Malaysia seems to only require such notice where the data user proposes to change the purpose of use to one different from the original purpose of collection.

Consent to collection, and definitions of consent

Half of the Asian laws explicitly require consent for collection from the data subject, and other forms of processing. Others do not, even though they usually require notice. Notice requirements to data subjects may often mean that there is implied consent to the purpose of collection. South Korea, Taiwan, Macau, and Malaysia do explicitly require consent before collection, with few and relatively narrow exceptions. The Philippines' law, while ostensibly requiring consent, has so many exceptions that consent is just one of many methods by which processing may be legitimate. China and Vietnam require consent (in the consumer and e-commerce contexts). It is not part of the banker's duty to the customer to obtain consent from the customer before collecting information about him or her.

Definitions of consent vary greatly, affecting not only collection, but also use and disclosure of personal data. Macau requires 'unambiguous consent'. Taiwan requires written consent. The Philippines requires that consent be a 'freely given, specific, informed indication of will' and that it be 'evidenced by written, electronic or recorded means', which leaves open the possibility of an express 'opt out' but not implied consents. Hong Kong often requires 'prescribed consent', which must be express, and can be withdrawn. The South Korean law concerning consent is unusually strict in that it requires not only writing but (i) separate consents for each item requiring consent (i.e. 'unbundling' of consents); (ii) segregation on consent forms of those items that require consent and those that do not ('unbundling' non-

[70] Kuner says 'the data controller must specifically inform the data subject of the purposes for which data are being collected': Kuner, *European Data Protection Law*, p. 100.

[71] See details in the country chapters in Part II of Greenleaf *Asian Data Privacy Laws*.

consents). Malaysia also requires unbundling of consents. This lack of consistency, even though express consent is most commonly required, is likely to cause difficulty for companies attempting to do business across multiple Asian jurisdictions, and it might be easier to adopt a standard approach of explicit unbundled consents.

The fourth exception to *Tournier* (discussed below) allowing disclosures by a bank (not internal uses), is express or implied consent by a customer. Consent need not be written; it can be implied, for example, from notorious banking practice or a practice that the customer is made aware of.[72] Under the statutory bank secrecy regime of Singapore, consent must be written but there is some debate about what qualifies as written consent.[73] As discussed above, the forms of consent required by data privacy laws will often be more strict than bank secrecy laws, and in such cases banks will have to comply with both standards prevailing in their jurisdictions.

Lawful, fair, and non-intrusive collection

Laws in almost all Asian jurisdictions follow the minimum requirements that collection must be by lawful means, and by fair means (which is a substantive limitation going beyond other existing laws), with only India and Malaysia omitting these minimum requirements. China only includes them explicitly in its Guidelines, but some of its laws refer to general principles of fairness and good faith. In Hong Kong, 'fair' has been interpreted by a tribunal to include 'non-intrusive' means in a case concerning paparazzi. The scope of the fair processing requirements in other jurisdictions is less clear. There are no equivalent requirements in the bank's duties to customers.

'Openness' requirements – particularly privacy policies

The minimum requirement of the principle of 'openness' (as the OECD described it), is that any person should be able to find out about personal data processing practices, whether or not they are a data subject. It is found in an explicit form in the legislation of only seven of the 11 Asian jurisdictions. However, all Asian laws except those of the Philippines and Japan require a published privacy policy.

Use & disclosure restrictions vs *Tournier* exceptions

The banker's common law, contractual duty of secrecy is not absolute, and its exceptions were said by Bankes LJ in *Tournier* to be classified under four heads: '(a) where disclosure is under compulsion by law; (b) where there is a duty to the public to disclose; (c) where the interests of the bank require disclosure; (d) where the disclosure is made by the express or implied consent of the customer.' These exceptions will be compared below to their equivalents in data privacy laws. The compulsion by law ('statutory') exceptions in data privacy laws to the use and disclosure principles are most likely to be of relevance to banks, because they go beyond the question of 'compatible uses' which is first discussed.

Secondary uses/disclosures based on 'compatibility', etc.

The bank's duties under *Tournier* limit only disclosures ('secrecy'), not internal uses by the bank which may be different from the purposes for which they originally collected the information. Data privacy laws go further, limiting internal uses (as well as disclosures) in various ways linked to the purpose of collection. In other words, the original purpose of collection of personal data is the starting point in determining what uses may be made of the data, including disclosures of it. This is sometimes called the 'finality' principle of data privacy

---

[72] *Turner v Royal Bank of Scotland plc* [1998] EWCA Civ 529; [1999] 2 All ER (Comm) 664.

[73] See Booysen, Chapter [].

laws, and exceptions to it are expressed in various ways.[74] All Asian data privacy laws start from requiring personal data to be used or disclosed only for the purpose for which the personal data was collected, but then allow a spectrum of 'secondary uses' (of varying widths) to be added, by formulae such as 'not incompatible or 'reasonably expected' uses or disclosures. All of the Asian data privacy laws therefore include to some extent the principle of 'finality,' meaning a limit to the uses that can be made of collected data based on the original purpose of collection.

The main issue becomes what exceptions to collection-purpose-based 'finality' are allowed, described as 'secondary' uses or disclosures. In Asia quite a range of wordings are used to indicate allowed secondary uses.[75] The differences (if any) between the meanings of these terms is speculative in the absence of decisions interpreting them, but it seems likely that a considerable range of differences will emerge.

For example, the Canadian Privacy Commissioner determined that a couple's personal information (closure of an account and reasons for closure) was disclosed by one bank to another for a purpose that a reasonable person would not find appropriate in the circumstances, even though the customer had signed a broad document consent to such disclosures.[76] A bank that sold details of its credit card accounts (information and liabilities) to another bank was in breach where it had not obtained the customer's consent – but another bank was not because it had obtained consent through an assignment clause in an agreement.[77]

Other examples of breaches include a Canadian bank which breached collection limitations ('over collection') by requiring a tax return and assessment;[78] an Australian bank allegedly used credit card transaction details to check on staff sick leave;[79] a Canadian bank inadvertently but wrongly disclosed details to a customer's mother (with the same name).[80]

---

[74] Both the basic and European principles allow additional ('secondary') uses/disclosures that are 'not incompatible' with the purpose of collection. In the EU, this very general criterion for secondary uses has been interpreted differently between member states, but is usually accompanied by requirements that data subjects be informed very specifically of the purpose of collection, thus limiting what can be regarded as 'compatible. See Kuner, *European Data Protection Law*, pp. 99–100.

[75] These include (from potentially least restrictive to potentially most restrictive) the wordings of 'not incompatible' (Macau), 'compatible' (the Philippines), 'reasonably expected' (Singapore), 'duly related' (Japan), 'directly related' (Hong Kong, Malaysia), 'in conformity with' (Taiwan), 'within the scope' (South Korea), for the 'purpose and scope announced' (Vietnam) and 'for the purpose for which it has been collected' (but with limited application) (India). China's more recent laws use a variety of wordings. In the Philippines, mere 'compatibility' does not seem sufficient unless the use/disclosure is also for 'legitimate interests' or within another exception. At the other end of the spectrum, in Malaysia, secondary disclosures are allowed where 'directly related' (and for other reasons), but secondary uses do not have to be 'directly related'. Singapore's Act does allow secondary use on the basis of purposes that a reasonable person would consider appropriate, but secondary uses will more often be based on 'deemed consent', lengthy schedules of exceptions, and other legislation. The overall position is too complex to be clear.

[76] PIPEDA Case Summary #2003-211: Bank accused of improperly disclosing overdraft information to another bank [2003] CAPrivCmr 113 < http://www.worldlii.org/ca/cases/CAPrivCmr/2003/113.html>.

[77] PIPEDA Case Summary #2006-350: Customers allege that sale of personal information by one bank to another occurred without knowledge and consent [2006] CAPrivCmr 17 < http://www.worldlii.org/cgi-bin/sinodisp/ca/cases/CAPrivCmr/2006/17.html>

[78] PIPEDA Report of Findings #2013-009: Bank over-collects client's personal information for credit increase [2013] CAPrivCmr 13 (28 May 2013) < http://www.worldlii.org/ ca/cases/CAPrivCmr/2013/13.html>.

[79] Bank allegedly using credit card transaction details to check on staff sick leave [1997] NSWPrivCmr 4 <http://www.austlii.edu.au/au/cases/nsw/NSWPrivCmr/1997/4.html>

[80] PIPEDA Case Summary #2002-100: Woman accuses bank of telling her mother about her bank account [2002] CAPrivCmr 94 < http://www.worldlii.org/ca/cases/CAPrivCmr/2002/94.html>.

Statutory exceptions to use and disclosure principles

Tournier provides that the contractual duty of confidentiality is overridden by the duty of both parties to submit to other legal requirements, including statutory requirements. There must be a legal requirement involving compulsion, not merely a demand or request from a government body. Such duties can arise outside statutes, such as the common law duty of a banker who is a witness in court to disclose in response to questions asked. Normally, only the requirements of local laws, not foreign laws, are relevant.[81] Statutory bank secrecy regimes tend to have similar qualifications, for example in Singapore and Switzerland.[82]

The statutory exceptions in data privacy laws vary too widely to cover fully here.[83] Hong Kong has a typical range of statutory exemptions relevant to banks. There are exemptions from the principles of use limitation, and of subject access, where it is considered necessary to protect various public and social interests such as the prevention and detection of crime, and the remedying of unlawful[84] conduct. The exemptions only apply where complying with the privacy principles would prejudice the interests concerned. In Korea there are limited exceptions to the need for consent: where special provisions exist in other laws; where the data subject (or legal representative) is not in a position to give consent, or their address is unknown, and it is necessary to protect the interests of the data subject or a third party (but not the interests of the bank, the data controller). Taiwan allows broad exemptions from obtaining consent or informing persons where collection, processing or use is made for purposes of public interest (undefined) and also meets other criteria. Malaysia provides a very broad exemption for any processing by commercial organisations 'for the purpose of carrying out regulatory functions' where application of the Act would be likely to prejudice those functions. It also has six general exceptions from the requirement of consent, which result in a broad 'authorised by law' type of exception for all forms of processing (except where sensitive data is concerned). The Philippines has very similar exemptions relating to functions of public authorities and assisting investigations.

While there is some degree of consistency across Asia in relation to these statutory exceptions, particularly where uses to assist law enforcement are concerned, this should not be exaggerated, and each country has substantial differences from the next.

Broad exceptions based on the public interest or the interests of others

The most poorly-defined of the *Tournier* exceptions is 'where there is a duty to the public to disclose. Suggestions have been made that this would include where the customer's dealings indicated dealing with the enemy in time of war' or where there is a 'danger to the state'.[85] Lord Denning took a broader view that the exception 'should extend to crimes, frauds and misdeeds, both those actually committed as well as those in contemplation, provided always – and this is essential – that the disclosure is justified in the public interest'.[86] In 1989, the UK Court of Appeal tentatively accepted that such an exception could excuse a disclosure by a

---

81 See, for example, XAG v A Bank [1983] 2 All ER 464 and FDC Co Ltd v Chase Manhattan Bank NA [1984] HKCA 260 where foreign court orders were held not to be justification for disclosing customer's account details.

82 As discussed by Booysen and Nobel in Chapters [], respectively.

83 Details are in the relevant country chapters in Part II of Greenleaf *Asian Data Privacy Laws*.

84 'Unlawful' in this context includes civil wrongs. For example, witness statements collected for the purpose of possible criminal proceedings, were permitted to be disclosed to plaintiffs in a civil suit: *Lily Tse Lai Yin & Others v The Incorporated Owners of Albert House & Others* [2001] HKCFI 976.

85 See Tyree *Banking Law in Australia*, 6.2.4 for discussion.

86 *Initial Services v Putterill* [1967] 3 All ER 145 at 148.

bank in the UK to the US Federal Reserve that Libyan parties appeared to be moving funds in breach of US decrees freezing Libyan funds.[87] After the subsequent quarter-century of legislation requiring 'suspicion-based' bank reporting of money-laundering, potential terrorism, sanctions-avoidance, etc, it is easy to imagine that the *Tournier* duty would be readily found to include exceptions for such purposes.

In data privacy laws, similar exceptions are often found. The examples of Hong Kong and Taiwan are given above. Macau and the Philippines have narrower exceptions based on the EU exception for protection of the legitimate interests of others (as distinct from the public interest), but only if they are not overridden by interests in protecting the fundamental rights of the data subject.[88]

Exceptions based on the interests of the bank

Another *Tournier* exception is 'where the interests of the bank require disclosure'. This is regarded as including where the bank has initiated legal proceedings, and where a guarantor seeks information about the account of a primary debtor, although the extent of this exception is unclear.[89] In data privacy laws, such exceptions based on the interests of the data controller (the bank in this instance) are very unusual.

Exceptions based on consent

One of the *Tournier* exceptions is 'where the disclosure is made by the express or implied consent of the customer.' Consent must be informed, so customers must be aware of the banking practice relied upon.[90] The practice of 'banker's references' has led to considerable dispute concerning when such references can be said to be based on implied consent, and one point of view is that such practices are more safely based on express consent, or at least on the giving of notice to the customer. [91]

In data privacy laws, although consent is always an allowed ground for change of use or for new types of disclosure of personal data, the extent of disclosure and other conditions for valid consent vary, as discussed earlier. The South Korean requirements for such consent are strict and require disclosure of identity of recipients, and of the consequences of refusing consent.

Exceptions based merely on notice

The minimum principles for data privacy laws require that every change of purpose must be 'specified'. South Korea has detailed notice requirements when consent is sought for change of purpose. The minimum principles do not state that giving notice is sufficient in itself (as an exception to the finality requirement) to be the basis of a change of purpose. However, Japan allows new disclosures (unrelated to the purpose of collection) after notice is given on a website, with an opt-out allowed, but this does not apply to new secondary uses by the data user. It is therefore questionable whether Japan's law complies with the basic principles. Malaysia has exceptions for disclosure which depend on notice, but also require being 'directly related' to the purpose of collection. *Tournier* and statutory regimes, such as Singapore's, do not include an exception based merely on notice.

---

[87] *Libyan Arab Foreign Bank v Banker's Trust Co* [1989] QB 728, per Staughton J.

[88] FRA, *Handbook on European Data Protection Law*, pp. 84–90; see EU Directive, art. 7(f).

[89] See Tyree *Banking Law in Australia*, 6.2.5 for discussion.

[90] *Turner v Royal Bank of Scotland* [1998] EWCA Civ 529.

[91] See Tyree *Banking Law in Australia*, part 6.3.

Restrictions on direct marketing uses

Tournier does not impose restrictions on a bank's internal uses of information it holds, but data privacy laws will usually do so where the use is for marketing purposes. Singapore's bank secrecy regime was, notably, amended after the passing of its data protection law, to stop the marketing exception.[92] In the EU, the right to object to personal data being used for direct marketing is required to be able to be exercised before data is transferred to third parties,[93] not only as the data subject's *ex post facto* response to a direct marketing communication. Seven Asian laws take an approach at least as strong as that of the EU.[94] Overall, this is one of the strongest implementations of a 'European' principle across Asian jurisdictions. Hong Kong (after the 2012 amendments) and South Korea now go further: if consent to collect data is being obtained for any marketing purposes, the data subject must be told this, and their consent to that use obtained, so 'opt-in' is in fact required. Complaints of breaches are common. In Hong Kong, putting opt-out requirements in small print at the back of an advisory letter was not sufficient notice[95] in a case where a A Hong Kong bank failed to follow the opt-out procedures in the HK law.[96]

International dimensions of banking disclosures

The issues surrounding the transfer of personal data between countries, and the overseas operation of data privacy laws, are very contentious, and have generated a substantial literature.[97] The issues can only be summarised here but are discussed elsewhere at length.[98] Overall, in Asia, it has been argued that only in South Korea and Macau can the overall requirements be described as somewhat strict on businesses involved in data exports, and protective of data subjects.[99] Almost everywhere else data subjects are generally in a very weak position, although the position in Singapore is complex.[100]

Does the law of the controller's jurisdiction assert extraterritorial operation? In Asia, explicit assertions of extraterritorial application are found in only four data privacy laws, but it is a more difficult question whether there are implied assertions of extraterritorial application. Only in South Korea, China, and Vietnam does there seem to be no likely extraterritorial scope.

---

[92] As discussed in Booysen, Chapter [].

[93] FRA, *Handbook on European Data Protection Law*, p. 119; see art. 14(b) of the EU Directive.

[94] The European-influenced principle of a right to opt-out from direct marketing are found in Macau, Hong Kong, South Korea, Malaysia, Taiwan, and Vietnam. Both of China's highest level laws may require similarly. India has a weak form of opt-out through withdrawal of consent, and Japan a different but equally weak opt-out through notices on websites. Only Singapore and the Philippines do not require either opt-out or opt-in procedures (no matter how weak), so in those countries the only limit is whether a particular form of marketing is allowed as a secondary use of the personal data.

[95] A and Financial Institution [2012] AICmrCN 1 <http://www.austlii.edu.au/au/cases/cth/AICmrCN/2012/1.html>

[96] Collection and Use of Customers' Personal Data by Industrial and Commercial Bank of China (Asia) Limited in Direct Marketing [2011] HKPCPDIR 5; R11-7946 < http://www.worldlii.org/eng/hk/other/pcpd/IR/2011/5.html>

[97] For leading examples, see Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, 2013) and Dan Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing, 2013).

[98] See Greenleaf *Asian Data Privacy Laws* (OUP 2014), Chapter 17 part 6 'Comparing the international dimensions of data privacy laws', pgs. 497-501.

[99] See Greenleaf *Asian Data Privacy Laws*, pgs. 499-500.

[100] Greenleaf, G 'Regulations bring Singapore's data privacy law into force' (2014) 130 *Privacy Laws & Business International Report,* 1-4.

Under what conditions are transfers to a foreign jurisdiction allowed, whether to contracted data processors, or to third parties? Four jurisdictions, Hong Kong, Japan, Vietnam, and the Philippines, have no effective limitations, and China's restrictions are based only on Guidelines as yet. Overall, the other Asian jurisdictions with data privacy laws have a fairly low level of restrictions on personal data exports, but with much variation.

Can the data subject enforce a contract against the recipient of exported data? In most Asian jurisdictions data subjects can (in theory) enforce contracts made between a local data controller and a foreign processor which are expressed to be for the benefit of data subjects, such as are required (for example) in Standard Contract Clauses for data exports from EU countries.[101] However, some common law jurisdictions, have a doctrine of privity of contract which prevents third parties (data subjects) for whose benefit contracts are made from enforcing those contracts. Any form of 'standard contractual clauses' are therefore useless as a form of protection providing rights to data subjects, in relation to exports from those jurisdictions. Singapore and Hong Kong have reformed the doctrine of privity of contract along the lines of the UK reforms, to allow such enforcement in some circumstances.

Security and data breach notification vs safe custody duties

One of the most likely areas of vulnerability with serious consequences for banks is breaches of the security of customer information, with possible additional liabilities to notify data breaches, and even to pay mandatory compensation to each customer whose details are disclosed.

Banks' duties of secrecy of account information and other information about account-holders, and duties of safe custody of documents (as a bailee), are each capable of breach. In some countries the duty may be absolute, but in other countries such as Australia, negligent breach may be required, with the probable standard of care being that of a 'reasonable banker in all the circumstances'.[102]

Data privacy laws in all jurisdictions require security safeguards, which must usually be against 'loss or unauthorised access, destruction, use, modification or disclosure' (minimum requirements), and only state the requirements in such abbreviated form. The standard of care required is sometimes phrased as requiring 'appropriate' measures, which is the European terminology[103] (Macau and Taiwan), or to take 'reasonable' steps, which is the OECD terminology. Some jurisdictions have an arguably stronger formulation such as 'necessary and proper steps' (Japan), 'whatever is necessary' to secure data (South Korea), or other formulations such as 'practical steps' (Malaysia). Detailed security requirements may also be specified (e.g. South Korea, Malaysia, and Macau), and are likely to be more important than the words used to specify a standard. The Philippines has special security provisions for government agencies holding sensitive data (such as data pertaining to ethnicity, religion and health), and requirements that contractors holding such data must register with the DPA.

Two examples concerning banks are illustrative. In the UK, a monetary penalty notice was served on the Bank of Scotland after customers' account details were repeatedly faxed to the wrong recipients. The information included payslips, bank statements, account details and

[101] See Chapter 2, section 3.1 Greenleaf *Asian Data Privacy Laws*.

[102] See Tyree *Banking Law in Australia*, part 6.6.

[103] FRA, Handbook on European Data Protection Law, pp. 95–6.

mortgage applications, along with customers' names, addresses and contact details.[104] In an Australian case, the complainant and his wife applied for a loan with a bank, and provided the bank with all their financial details (including tax returns). The bank's branch office then faxed these details (plus comments on the credit worthiness of the complainants) in a nineteen page fax to its head office. Unfortunately, the fax was incorrectly sent to an unrelated third party. The bank responded to the complaint by directing all its branch offices to ensure that the head office fax number was stored in the autodial memory of every branch fax machine and paid $500 each to the complainant and his wife for their embarrassment.[105]

Data breach notification

The traditional duties of banks have not explicitly required them to advise their customers, or governments, if the security of customer information is compromised. Under data privacy laws, requirements to issue compulsory data breach notification (DBN), can be a considerable sanction because of their potential effects on the reputation and financial situation of a bank or other data controller. Various jurisdictions in the USA have had DBN requirements for some years. They exist in the laws of some European jurisdictions, and are compulsory under EU law for telecommunications providers.[106] They are now required under the revised 2013 OECD Guidelines.[107] In Asia, DBN is required by four laws. In South Korea, the Philippines, and Taiwan, individuals likely to be affected must be notified of data breaches. In China, the Philippines, and South Korea (when affecting more than 10,000 data subjects) the DPA or relevant ministry must be notified. There are no DBN provisions in the comparatively recent Singaporean and Malaysian laws, the revised Hong Kong law,[108] Macau's law (which reflects the state of EU law a decade ago), India's legislation, or Japan's newly-revised law.[109] The Australian government released a discussion draft Bill for mandatory data breach notification in December 2015. An Australian example that prompted notification under its existing voluntary scheme is where a superannuation provider allowed data on 568 members to be downloaded from a website as a result of lack of adequate security measures.[110]

Compulsory compensation for data breaches

Under the common law bank secrecy regime of *Tournier*, damages are recoverable for breach of the duty of secrecy.[111] Under statutory regimes, the availability of damages will depend on the legislation, although in some cases, this may be unclear.[112] Data privacy laws in Asia are very variable in whether data subjects are able to seek compensation through court

---

[104] Bank of Scotland (Monetary penalty Notice) [2013] UKICO 2013-7 < http://www.bailii.org/uk/cases/UKICO/2013/2013-7.html>

[105] Bank faxes details to wrong number - Section 18N [1995] PrivCmrA 12 <http://www.austlii.edu.au/au/cases/cth/PrivCmrA/1995/12.htm>

[106] FRA, *Handbook on European Data Protection Law*, pp. 96–7.

[107] See Chapter 19, section 3.3, Greenleaf *Asian Data Privacy Laws*.

[108] In Hong Kong, government agencies have reached agreement with the privacy commissioner to notify him immediately of such breaches, but this does not apply to the private sector, despite the recent revisions to its law.

[109] Greenleaf, G 'Japan: Toward international standards – except for 'big data' (2015) 135 *Privacy Laws & Business International Report,* 12-14 <http://ssrn.com/abstract=2649556>. In Japan, ministerial guidelines require notification to the relevant ministry, the basis of a quasi-voluntary data breach notification system.

[110] First State Super Trustee Corporation: Own motion investigation report [2012] AICmrCN 4 <http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/AICmrCN/2012/4.html?> No compensation available for Own Motion Investigations until 2014.

[111] See Stanton chapter in this book; also Tyree Banking Law in Australia, part []

[112] See, for example, Booysen chapter in this book.

proceedings,[113] and none allow compensation to be awarded by data protection authorities (in contrast with Australia). The most liberal compensatory provisions where damage results from data breaches, are in amendments to Korea's *Credit Information Act* in March 2015, which provide for punitive damages of up to 3 times the damage caused by personal credit information being lost, stolen, leaked, fabricated, or damaged due to the relevant business' wilful misconduct or gross negligence. More significantly, they provide for statutory damages of up to US$3,000 (KRW 3 million) per data subject whose personal credit information was stolen, lost, leaked, fabricated, or damaged due to the relevant business' wilful misconduct or negligence, without need from proof of damage. Such provisions are likely to be extended in Korea to all data controllers. It is possible that this approach may spread to other jurisdictions.

Access, correction and other new customer rights

Banker-customer law does not generally give customers a right to access the files banks hold on them. In data privacy laws, user access and correction rights are found in all Asian jurisdictions except China.[114] Taiwan has an unusual and strong provision that user rights 'may not be waived in advance nor limited by special agreement', and other jurisdictions are also reluctant to allow such rights to be waived or restricted. For example, a New Zealand bank's claim of 'trade secret' was rejected as a basis for limiting statutory access.[115] A Canadian bank has also failed in its attempts to rely on exemptions to limit access rights of employee.[116]

Access, and data portability

South Korea exemplifies the broadest access rights, requiring access not only to the content held, but also the purpose of collection and use, the retention period, details of disclosures to third parties, and details of consents by the data subject. At least Singapore, Hong Kong, the Philippines, and Taiwan also require disclosures to third parties in access requests (requiring specific request in Singapore). The Philippines' novel contribution to Asian data privacy laws is the right to obtain a copy of your file in a commonly used machine-readable form, anticipating proposals for reform of the EU Directive. Macau requires the DPA to be informed of some types of refusal of access. Exceptions to rights of access and correction vary a great deal.[117]

Some jurisdictions such as Hong Kong allow a data user to charge a reasonable but not excessive fee for complying with a data access request. Its DPA has held some fees to be excessive,[118] such as where a bank set up a new fee structure intending to charge all customers a flat-rate fixed fee of HK$200 (US$25) for complying with a data access request to obtain copies of their personal data in the custody of the bank, but was held to be permitted to recover only the labour costs and actual out-of-pocket expenses incurred in locating,

---

[113] See Greenleaf Asian Data Privacy Laws, Chapter 18, part 3.5 'Access to judicial remedies by data subjects'.

[114] All of China's data privacy laws primarily address the obligations of the administrator of personal information, and do not clearly state the rights of data subjects. 2013 Guidelines (not a law), for the first time, clearly assume and imply rights of access and correction.

[115] Bank Refuses Couple Access To File Claiming Trade Secret - (Case Note 36631) [2003] NZPrivCmr 14 <http://www.nzlii.org/nz/cases/NZPrivCmr/2003/14.html>

[116] PIPEDA Report of Findings #2013-004: Bank provides former employee with insufficient access to his personal information [2013] CAPrivCmr 17 <http://www.worldlii.org/ca/cases/CAPrivCmr/2013/17.html>

[117] The details are in the relevant country chapters in Part II of Greenleaf *Asian Data Privacy Laws*.

[118] See PCPD *Principles*, pp. 87–8 for detailed considerations.

retrieving, reproducing, and sending the requested data to the requestor based on the work involved being done by clerical or administrative staff. The bank failed to establish it had taken this approach, and was found to have imposed a fee structure that was liable to be excessive. The Bank abandoned the proposed fee structure before implementing it.[119]

Corrections and notifications

Half of the Asian laws do require notification of corrections to third parties who have had access to a person's file: Hong Kong, Singapore, Macau Taiwan, and the Philippines. Macau extends this to blocking and erasure, and requires third parties to do likewise. In South Korea, correction (and deletion) requests must be decided within 10 days, and if denied the reasons (including information about how to appeal) must be provided in a standard outcome notice, but leaves it up to the data subject to inform third parties. Where a correction is refused, the data subject is explicitly entitled to add their own version of the situation to their file, in Hong Kong, Malaysia, and Taiwan, although there is variation in what may be added. Other laws may allow this by implication of the data quality principle. This does not seem to occur in Japan.

Accuracy and completeness

All Asian data privacy laws impose duties on the bank to the data subject that personal data must be accurate and complete (relative to the use of the data), with wording varying considerably between jurisdictions. In banking law, there is a contractual duty on the bank to exercise reasonable care and skill to give accurate and complete information, when giving 'bank references' (or similar disclosures to third parties like credit bureaus).[120] The duty under data privacy laws is not restricted to such situations, and could apply in situations where there is, for example, a statutory duty to disclose to a government body, but the personal data held by the bank is inaccurate or incomplete, and harm to the customer results.

Deletion and blocking of use—automatic and on request

Automatic (i.e. non-request) deletion or anonymization of data once the reason for its collection is completed, is required in all Asian jurisdictions except Japan, Vietnam, and China.[121] The Philippines provisions have many exceptions and are ill-drafted. In Singapore the provision for deletion of data will be difficult to enforce, due to the complexity of proving that all legitimate business purposes have expired.[122] India's provision has multiple defects.[123] There is often ambiguity, as in Taiwan, about whether data must be deleted, or can be anonymized.

Deletion of data on request, including data provided by third parties, is provided in South Korea. This is close to a 'right to be forgotten' in its implementation. In Japan there is a vague provision allowing data subjects to request deletion, but it is not clear when the data controller can refuse to do so. A right to block the use of data is found in South Korea, Macau, Malaysia, the Philippines, and Taiwan. India allows consent to use information to be withdrawn, which implies that use is blocked, but not deletion. Hong Kong allows 'prescribed

---

[119] PCPD, 'Bank Imposing Fee at a Flat Rate for Complying with a Data Access Request' (PCPD s. 48(2) Report R10-5528, 24 February 2010).

[120] See Tyree *Banking Law in Australia*, part 6.3.2. The *Hedley Byrne* principles only protects the recipient of a bank reference against negligence, not the data subject: see 6.3.3.

[121] It is not required by the minimum data privacy principles, but is required by European principles.

[122] See Greenleaf, *Asian Data Privacy Laws*, p. 301.

[123] It only applies to sensitive information and only prohibits retention of information beyond when it may lawfully be used, which is not the same as when its purpose of collection has expired

consent' to collect data to be withdrawn, implying a right to block use of data originating from the data subject. There are no such provisions in China or Vietnam. South Korea is also unusual in having a specific provision that data subjects must be informed of the transfer of their personal information as the result of sale of a business in whole or part, and that they have a right to opt-out (withdraw consent) from their personal information being transferred.

Conclusion

There is common ground between bank secrecy and data privacy regimes, but the differences are complex and occur at many points, resisting any simple comparisons. In a few respects, *Tournier* duties of banks may be broader than those arising from data privacy laws, such as in their application to non-natural persons, and their duties of safe custody. In most respects, however, it is data privacy laws that impose more strict obligations, including: limits on personal data collected; a narrower range of allowed disclosures; data breach notification requirements; and access and correction regimes. Usually, banks will have to comply with both traditional duties of secrecy, and with data privacy regimes and their stricter and broader requirements, subject to specific statutory exceptions. Both regimes are subject to the overriding requirements of AML-CTF laws.

Now that data privacy laws are becoming ubiquitous across the world, and with relatively consistent standards, as suggested earlier, banks everywhere will increasingly have to take into account data privacy laws, in addition to their traditional duties. The breadth of obligations imposed by these laws, while often in parallel with traditional duties, are generally of much broader scope, and will require new accommodations in banking practice, particularly for banks with multinational operations.