

Global data privacy in a networked world

Graham Greenleaf, University of New South Wales

For publication as a Chapter in Brown, I (ed) *Research Handbook on Governance of the Internet*
Cheltenham: Edward Elgar, forthcoming 2012 – please cite published version. (1 September 2011)

Contents

Global data privacy in a networked world	1
Introduction: Technological challenges and ‘Internet governance’	2
Data privacy laws: Effectiveness and alternatives	2
Evolution	3
Persistence, expansion and consistency of data privacy laws	4
Global expansion of national data privacy laws	4
Countries without data privacy laws, and their significance	5
United States exceptionalism and its significance	6
Influence of international agreements, and ‘European’ standards	7
The EU’s influence and its future intentions	7
The failed APEC alternative	8
ECOWAS and other regional agreements on data privacy	9
Data privacy principles	10
Nature and limits of data privacy principles	11
Core data privacy principles	11
Data export limitations and ‘adequacy’	12
The contested principle of ‘accountability’	14
Emergent data privacy principles	15
Data privacy enforcement	16
Standards for enforcement mechanisms	16
The poor enforcement record of most DPAs	17
Emergent mechanisms for enforcement	17
New challenges of a networked world: Can data privacy laws cope?	18
Conclusion – The trajectory of global data privacy regulation	19
Appendix: Global Table of data privacy laws	22
References	25

Introduction: Technological challenges and 'Internet governance'

This Chapter¹ provides an overview of the state of global data privacy law (also called 'data protection' and 'information privacy') as at mid-2011, with an emphasis on the extent to which such laws are able to deal with new technological challenges associated with the networking of the world resulting primarily from the development of the Internet, particularly since 1995. Special attention is given to two most likely indicators of the directions in which global data privacy will develop: the EU Commission's proposals for expansion of data privacy law set out in the report 'A comprehensive approach on personal data protection in the European Union' (EU Commission, 2010); and the recent rapid expansion of new data privacy laws outside Europe.

The context of the new technological challenges is summarised in a report to the EU Commission (Korff, Brown and others, 2010) as follows:

We have seen dramatic technological change since the European Commission first proposed the Data Protection Directive in 1990. The Internet has moved out of the university lab into 56% of European homes and 95% of OECD businesses. Computer processing power has continued to follow Moore's Law, with transistor density doubling every 18-24 months – around one thousand-fold in the last two decades. Computer storage capacity and communications bandwidth have both been increasing even more quickly, doubling every 12 months and hence a thousand-fold each decade. These exponential increases have radically increased the ability of organisations to collect, store and process personal data. The physical environment is now saturated with sensors such as CCTV cameras and mobile phones, with biometric and electronic identifiers used to link data to individuals. In the digital world almost every communication and Web page access leaves behind detailed footprints. The Internet and mobile information appliances allow large quantities of personal data to be trivially moved between jurisdictions. Data mining tools attempt to find patterns in large collections of personal data, both to identify individuals "of interest" and to attempt to predict their interests and preferences. New multinational companies have sprung up around these technologies to service a global customer base, with smaller enterprises outsourcing employee and customer data processing to developing world companies.

In a book dealing with 'Internet governance', it is important to recognise that there is no global organisation 'governing' data privacy which is in any way equivalent to, say, ICANN in the field of domain names and numbers, nor as yet any global treaties equivalent to the importance of the Berne Convention or the WIPO Copyright Treaty in the field of copyright. Also, data privacy as a matter of national legislation and international agreements pre-dates the mid-1990s' rise to significance of the Internet. Consequently, this chapter deals largely with national laws, and with pre-Internet international agreements. To the extent that there is any consistent form of 'global governance' in relation to data privacy, we will see that it comes from a combination of various international agreements, a particular mechanism encouraging consistency (the 'adequacy' criterion in the EU data protection Directive, 1995), and the concomitant emulation of European standards outside Europe.

The focus of this chapter is on legal instruments (and to a lesser extent the agencies implementing them) at the national level, and the international agreements influencing them, and not with self-regulatory instruments or regulation by technology (code), acting outside of legislative structures (for which see Bennett and Raab, 2006, Chs 6 and 7).

Data privacy laws: Effectiveness and alternatives

Data privacy laws essentially comprise a set of enforceable data privacy principles (based on the 'life cycle' of personal data: collection, accuracy, security, use, disclosure, access, deletion etc) and an enforcement structure, almost always involving a data privacy authority (usually called a 'Data Protection Authority' or 'Privacy Commissioner') as the first point of enforcement. The standard features of both principles and enforcement are discussed later. 'Privacy' is a broader interest than 'data privacy' and includes the protection of such interests as bodily integrity, solitude and freedom from observation, that do not necessarily involve issues concerning personal data, but the two increasingly overlap because of pervasive data collection.

Whether data privacy laws can sufficiently protect privacy in a networked world is an open question, but they are the legal instrument most capable of so doing. Other forms of legal protection (privacy torts, breach of confidence (both general principles and statutory rules), constitutional rights, surveillance limitation laws, consumer protection laws etc) give intermittent protection in some countries (and sometimes very effectively in specific cases) but do not provide the thorough and evolving protection provided by sets of data privacy principles. The fact that these alternatives are not discussed here does not diminish their importance in particular situations in particular countries.

Similarly, international human rights agreements sometimes create rights, or require creation of rights at national level, which sometimes protect privacy. Some general privacy rights have been employed by many courts in the protection of privacy and less frequently to specifically protect data privacy. The best examples are Article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1967) and particularly Article 8 of the European Convention on Human Rights. The effectiveness of these protections must not be ignored, and they do provide a basis in human rights law for data protection, but they have not yet been interpreted to encompass all aspects of data privacy, and often fall short of what is provided in specific data privacy instruments (Bygrave 1998 p247, 2010 p181). However, the EU's new constitutional instrument, the Charter of Fundamental Rights of the European Union, recognises a right to protection of personal data as a separate human right from the broader right of protection of privacy, the first time this has occurred in a human rights instrument (Bygrave 2010, p182).

The effectiveness of data privacy principles comes as much from their ideological effect and their global nature as from their enforcement (which is often lacking). Forty years of data privacy laws have created a language of data privacy, and a set of ethical standards to which most companies and governments feel obliged to at least give lip service. Attempts to break the power of this discourse by creation of alternative language/ethical standards, particularly the push for 'accountability' (discussed later), have failed as yet but are a continuing threat to the hegemony of conventional data privacy principles. Consequently, it can be argued that the most important form of 'self-regulation' in the area of data privacy is simply that many businesses and government agencies internalise the norms of data privacy principles once they are enacted and observe legislation to a significant extent even in the absence of effective enforcement activities. Survey data from Australia (cited in Greenleaf, 2008a) and Hong Kong (cite in McLeish and Greenleaf, 2008, p251) give some support for this proposition. In this fundamental sense there has indeed been a good deal of self-regulation in privacy protection.

There is very little evidence, from what we have seen in the last forty years, that any non-legal constraints will prove effective against business and government self-interest in expanded surveillance: this applies to voluntary self-regulation (through codes of conduct, standard-setting, privacy seals, or spontaneous adoption of privacy-enhancing technologies (PETs) or privacy-by-design), the force of competition, or the adoption by consumers of PETs and counter-surveillance technologies. Bennett and Raab (2006, Chapters 6 and 7) survey most of these approaches and find little significant evidence of their success unless they are integrated into a data privacy regime. In that case they become 'co-regulation' supported by legal requirements, not 'self-regulation', and may be more effective though studies are still lacking.

Evolution

The notion of data privacy, while it has held a consistent core for about 40 years, is not static. New principles continue to emerge and become absorbed in new or amended data privacy legislation, the most notable recent example being 'data breach notification'. Other emergent principles include data tracking restrictions, the anonymous transactions right, and the 'right to be forgotten', though they can usually be seen as specific implications of already existing general principles. New methods of enforcement are also become part of the 'standard kit' of DPAs and data subjects (eg

representative complaint mechanisms are spreading; ‘data breach notification’ is as much an enforcement mechanism as a principle). But these occur within the framework of the accepted notion of ‘data protection’ (or ‘data privacy’ as used here).

Persistence, expansion and consistency of data privacy laws

Since Sweden’s *Data Act* of 1973 (the first national legislation to include most elements of what we now consider to be a data privacy law) legislation to protect privacy in relation to personal information has evolved in a largely consistent fashion across the world, with few major exceptions remaining.

Global expansion of national data privacy laws

The global rate of development of data privacy laws is accelerating, their geographical scope expanding, and their consistency increasingⁱⁱ. As at mid-2011 there are 75 countries (or otherwise independent legal jurisdictions) with data privacy laws, as detailed in the Appendix to this chapter. In a handful of cases (two Special Administrative Regions of China and five British dependent territories) these are not countries, but are largely autonomous entities with their own distinct legal systems (states or provinces of countries are not counted). By a ‘data privacy law’ is meant a law with a substantially complete set of data privacy principles which at least approximate minimal international standards (as in the OECD Guidelines (OECD, 1980) or Council of Europe Convention (CoE, 1981)), and a mandatory legal enforcement mechanism (not just self-regulation or guidelines). To be counted as such, a data privacy law must cover most of a country’s private sector, not merely a few sub-sectors like credit reporting, health or financial information (eg Dubai), and not only the public sector (eg Thailand; USA). In almost all cases, data privacy laws do cover the national public sector as well as the private sector (Malaysia and India are exceptions). Some other countries (eg Canada) have separate laws for their public and private sectors. Almost all data privacy laws establish some form of specialised ‘data protection authority’ (DPA), variously named and with differing degrees of independence, with at least the power to investigate individual complaints (but with widely-varying powers of enforcement, or alternative avenues of enforcement), and the ability to have some input into the policy-making process. From 75 jurisdictions, Russia, Chile, Colombia, the Kyrgyz Republic, India, Japan and Taiwan are among the few remaining exceptions with no DPA.

The total number of new data privacy laws globally, viewed by decade, shows that their growth is accelerating, not merely expanding linearly: 7 (1970s), 10 (1980s), 19 (1990s), 32 (2000s) and 7 (1.5 years of 2010s), giving the total of 75. In the 1970s data privacy laws were a western European phenomenon (Sweden, Germany, Austria, Denmark, France, Norway and Luxembourg), and similarly in the 1980s (UK, Ireland, Iceland, Finland, San Marino and the Netherlands, and three UK territories), with Israel as the first non-European state in 1981 (Australia’s 1988 legislation was public sector only). Acceleration commenced in the 1990s, as most remaining western European countries (EU and EEA) enacted laws (Portugal, Belgium, Spain, Switzerland, Monaco, Italy and Greece). More significantly, with the collapse of the Soviet Union many former ‘eastern bloc’ countries enacted data privacy laws as part of their protection of civil liberties (Slovenia, Czech Republic, Hungary, Slovakia, Poland and Albania), and the first ex-Soviet-republics (Lithuania and Azerbaijan) did likewise. The spread outside Europe also started, with the first laws in Latin America (Chile) and the Asia-Pacific (New Zealand, Hong Kong and Taiwan).

In the 2000s the acceleration continued, with dramatic expansion in the former eastern bloc and Soviet republic countries (Latvia, Bosnia & Herzegovina, Romania, Bulgaria, Croatia, Estonia, FYROM (Macedonia), Moldova, Serbia and Montenegro), plus the tidying up of the remaining European states (Cyprus, Malta, Andorra, Liechtenstein, Gibraltar). Outside Europe, expansion accelerated in the Asia-Pacific (Australia, South Korea, Japan, Macao SAR) and Latin America (Argentina, Colombia, Uruguay). In the Americas, Canada and the Bahamas added further new

laws. Rapid development took place in Africa with new laws in Tunisia and Morocco (North African) and Mauritius, Cape Verde, Benin Senegal and Burkina Faso (Sub-Saharan Africa). The Kyrgyz Republic became the first country in Central Asia to legislate in 2008. In the first 18 months of this decade 7 new laws have been enacted (Faroe Islands, Malaysia, Mexico, India, Peru, Russia - more accurately, brought into force - and Ukraine), making this the most intensive period of data protection developments in the last 40 years.

Geographically, almost two thirds of data privacy laws are in European states (48/75). EU member states now make up little more than one third (27/75), even with the expansion of the EU into eastern Europe. There are data privacy laws in all 27 member states of the EU, and a further 21 laws in other European jurisdictions. Only a few European states remain without such laws, such as Georgia and Belarus. There are six laws in Latin America, with Brazil set to become the seventh (Palazzi, 2011). In the Americas are also the laws in Canada and the Bahamas (the only law in the Caribbean). In Asia there are now eight data privacy laws, with Singapore promising a ninth, and the other eight ASEAN states committed to improved privacy protection (but not specifically to legislate) by 2015 (Connolly, 2008). Both Australia and New Zealand have data privacy laws, but none of the Pacific Islands do so (the only region with no such laws). In North Africa and the Middle East, there are three such laws, and five in Sub-Saharan Africa. Further Acts are likely soon, with Bills progressing in South Africa and Ghana. The French-Speaking Association of Personal Data Protection Authorities (AFAPDP), and France's CNIL have both played key roles in developing expansion of data privacy in Africa. The Kyrgyz Republic law is the first in Central Asia, though Mongolia has laws covering many elements of data privacy (Greenleaf, 2011a). So there are 27 data privacy laws outside Europe.

For over two decades the annual rate of adoption of new data privacy laws has been increasing steadily, from an average of 1.75 per year in the second half of the 1980s, to 3.5 per year for the last five years. The regions of the globe that have such laws have also been steadily expanding. If the current rate of expansion in the 2010s continues, 50 new laws will result in this decade. Even on the conservative (and probably unrealistic) assumption that the 2010s will see no more data privacy laws than the 2000s, the number of countries with data protection laws will exceed 100 by the decade's end, with the majority of data privacy laws by then coming from outside Europe. In addition, many existing laws are being strengthened to keep up with rising expectations of privacy protection, international agreements, and the examples set by other countries (see the 'Latest' column in the Table).

There are other ways that expansion could be measured, say by the populations of the countries concerned, or by their GNP. These could show different trends, but reflection on the size and economic significance of the countries so far included makes it obvious that data privacy laws are more common in the world's larger and more economically significant countries. The recent inclusion of India accelerates this trend, as will the likely inclusion of Brazil in the near future. By any measure, data privacy laws are of increasing and accelerating global significance.

Countries without data privacy laws, and their significance

The most economically significant countries still lacking data privacy laws (on the definition adopted here) are the USA, China and Brazil. India has now adopted a data privacy law (Greenleaf, 2011b, 2011c, 2011d). The omission of Brazil is also expected to be remedied in 2011 (Palazzi 2011). Most other countries that do not yet have data privacy laws are of relatively low significance in international trade, though some countries with large populations are among them, particularly in sub-Saharan Africa (eg Nigeria), and in Asia (eg Indonesia). However, some regions of economic cooperation (eg ECOWAS, ASEAN, Mercosur) which have large populations in aggregate, may play an important role in international data privacy developments in future.

China is currently in what can be called the ‘warring states period’ of data protection, with numerous factions of the Chinese bureaucracy disputing the best way to deal with data protection issues. As yet it only has a limited patchwork of laws (including recent privacy protections in both criminal law and tort law), but there has been draft national legislation (Greenleaf, 2008) and recent draft ‘guidelines’ (Greenleaf, 2011) both of which point in the direction of data privacy laws. What will eventuate in China, and whether it will influence others, are still questions to which no-one has a convincing answer.

There is a strong correlation between democracies and data privacy laws: most democracies have them (or are likely to soon), and most authoritarian regimes do not. The examples from eastern Europe in the 1990s shows that data privacy laws can become aligned with democratic and post-authoritarian aspirations (Szekely 2008), as is also the case with South Korea (Park, 2008). In the African region of greatest expansion of data privacy laws, the chairman of the Economic Community of West African States (ECOWAS) stated in 2011 that ‘the region will never allow unconstitutional ascension to power’, reflecting a 2001 regional declaration on democracy and good governance (ECOWAS, 2011). It would not be surprising if data privacy as a form of human rights protection in North African states becomes a regional reality if the ‘Arab Spring’ of 2011 matures into newly democratic states. The high correlation is not surprising: democratic values help justify data privacy laws (Bygrave, 2002 Chapter 7, 2010); and the ‘watchdog’ aspect of data privacy laws and institutions are a good fit for recent theories of ‘monitory democracy’ with its multitude of watchdogs monitoring the public sphere (Keane, 2011, particularly Part III).

United States exceptionalism and its significance

The USA has many privacy laws and some effective enforcement, but no comprehensive privacy law in the private sector, nor much prospect of one, despite periodic calls for one from the major companies and Bills introduced into Congress. A recent report (Hoofnagle, 2010) asserts that ‘the US approach is incoherent, sectorally-based, and ... legislative protections are largely reactive, driven by outrage at particular, narrow practices’. ‘In [Federal] statutory law, privacy rights are found in the criminal code, the civil code, evidentiary law, family law, property law, contracts, and in administrative regulations. No single overarching statute even attempts to unify these interests in the diverse contexts in which “privacy” is used to frame some value’. However, says Hoofnagle, ‘[t]his has created a tension between state and federal governments, resulting in a levelling up of protections, because states (which tend to be more activist on privacy issues) can act where the US Congress is occupied with other issues’. As a result, there has been a profusion of innovative state laws in areas as data breach notification and laws to limit effects of identity theft.

The key limits in the US approach to data privacy can be seen from Hoofnagle’s analysis of the most important recent development in the USA:

But most relevant to the new challenges [of technology] is the “federal common law” being created on a case-by-case basis by the Federal Trade Commission (FTC). It is important to note that the FTC has adopted a more limited set of fair information practices than international authorities. The agency is concerned with notice, choice, access, security, and accountability. There has been almost complete inattention to the right of access, as the agency sees access as heightening security risks and potentially triggering a requirement to collect more personal data. In recent years, a heavy emphasis has been placed on security... Under it, a company can engage in maximum data collection, because the information is “private” so long as it remains secret and secure within the company’s systems.

He summarises the other main gaps in the privacy principles adopted across US laws as follows: ‘US privacy law typically allows businesses to use personal information for different purposes, including for marketing, without the data subject’s consent. This is because the sectoral system leaves many businesses unregulated... Just a handful of laws create explicit purpose limitations’; and ‘US privacy law generally does not have limitations on collection of personal information.

Collection limitation runs counter to the notion of most enterprises, which attempt to collect as much information as possible in transactions’.

However, US exceptionalism should not be confused with a schism in global approaches to data privacy. Increasingly, the position is that the USA is the only significant outlier attempting to defend providing data privacy protection by a patchwork of sectoral laws (with significant limits to their principles) and no national DPA as a key means of enforcement. The rest of the world is increasingly adopting a generally consistent set of principles and establishing a DPA as part of the enforcement mechanism. Other countries that have previously taken an approach similar to the USA are changing course: Mexico, Malaysia and Peru have enacted laws which are both OECD and EU-influenced, with a DPA; Singapore and the Philippines are likely to do similarly (Greenleaf, 2011). Japan and Taiwan have not yet adopted a DPA, but have enacted otherwise extensive data privacy laws. US attempts to impede the spread of data privacy laws in Asia and Latin America through APEC-supported alternatives (discussed later) largely appear to have failed.

The USA is best seen as a country with a unique, isolated and often inconsistent approach to data privacy, one that remains behind the rest of the world in some respects (particularly limits on collection and re-use), but which also often provides international leadership in relation to some principles (eg data breach disclosure, and other aspects of security) and in the deterrent effect of draconian examples of enforcement, particularly by the FTC. These differences are amplified by the core role it plays as the host or provider of numerous Internet-based personal information services which have global reach. The attempt to make US-based services accommodate the data privacy approaches of most other countries will continue to be one of the defining features of global privacy developments for years to come. Similarly, attempts by US companies and the US government to use their combined economic and political influence to limit development of data privacy laws in other countries will continue to be important, but are probably now on the wrong side of history.

Influence of international agreements, and ‘European’ standards

International agreements concerning data privacy have contributed a great deal to the development of consistency of national data privacy laws. From the start of the 1980s the non-binding OECD privacy Guidelines (OECD, 1980) and the first binding international agreement, the Council of Europe data protection Convention (CoE, 1981), both embodied privacy principles with similar substance but expressed in somewhat different language.

The EU’s influence and its future intentions

From the mid-1990s the European Union’s data protection Directive (EU, 1995) embodied a set of privacy principles consistent with, but somewhat stronger than, those in the OECD and CoE agreements. However, the Directive added much stronger enforcement requirements, including establishment of an independent DPA and a right to have disputes heard by the courts. Unlike either of the earlier agreements, it also required limitations on data exports to countries outside the EU which did not have ‘adequate’ privacy laws (discussed in more detail later). All of these standards set by the Directive have become recognised as the strongest international standard for data privacy.

Fifteen years later, the EU’s promotion of its standards is growing stronger, although it is not without critics. After reviewing the EU’s current data privacy legal framework through conferences, consultations and commissioned reports (including Korff and Brown, 2010), the EU Commission has concluded that ‘the core principles of the Directive are still valid and that its technologically neutral character should be preserved’, although it should be strengthened in various ways (EU Commission, 2010, 1), as discussed later. The European Commission is intent on expanding the global influence of its standards, and in fact seems to see them as ‘universal principles’ (EU Commission, 2011, 2.4.2):

Data processing is globalised and calls for the development of universal principles for the protection of individuals with regard to the processing of personal data. The EU legal framework for data privacy has often served as a benchmark for third countries when regulating data privacy. Its effect and impact, within and outside the Union, have been of the utmost importance. The European Union must therefore remain a driving force behind the development and promotion of international legal and technical standards for the protection of personal data, based on relevant EU and other European instruments on data privacy.

Furthermore, it is intent on strengthening both the Principles and the enforcement mechanisms of EU data privacy (EU Commission, 2010). ‘The Lisbon Treaty provided the EU with additional means to achieve this: the EU Charter of Fundamental Rights - with Article 8 recognising an autonomous right to the protection of personal data - has become legally binding, and a new legal basis has been introduced allowing for the establishment of comprehensive and coherent Union legislation ...’. The aim is to ensure ‘that the fundamental right to data protection for individuals is fully respected within the EU and beyond’ (EU Commission, 2010, 1). The final two words indicate the significance for the rest of the world.

Outside Europe, something approaching ‘European standard’ data privacy laws is starting to become the norm in a number of parts of the world. This trend is most noticeable in Latin America, with Mexico recently joining Argentina, Colombia and Uruguay with EU-style laws. All the recent laws in West and North Africa show strong EU influence. In the last two years, revised laws in Taiwan and South Korea have moved further in the EU direction, as have new laws in India and Malaysia (while also showing influences of the OECD Guidelines). New draft guidelines in China also point in the EU direction. Japan, Macau, Hong Kong, New Zealand (soon to be the second Asia-Pacific country after Canada found to be ‘adequate’) and Australia (where protracted law reform should strengthen its law) all have laws which show EU influences to some degree. Nowhere in the new Asia-Pacific laws is there any strong evidence of APEC influence.

The failing APEC alternative

From the start of its development in 2003 the APEC (Asia-Pacific Economic Cooperation) Privacy Framework (APEC 2005) has been the only significant international attempt to break the influence of the EU Directive. APEC has 21 member ‘economies’ in Asia (including China but not India), the Americas (including the USA) and Australasia. Through its Framework, which is not legally binding, APEC advocated an alternative approach which falls short of the ‘European’ standards set primarily by the EU Directive in four respects: (i) its set of principles can be described as ‘OECD Lite’ (Greenleaf, 2004), weaker than the Directive or most regional laws, and with no additions of value (Greenleaf 2008); (ii) a complete absence of any obligations to enforce the principles by law (self-regulation unsupported by legislation is acceptable for APEC), or even a recommendation for legislation; (iii) no complementary obligation of free flow of personal data in return for adoption of basic standards (at best, an encouragement of development of mutually-acceptable cross-border privacy rules (CBPR) by companies); and (iv) an ‘Accountability’ principle which is an incoherent substitute for data export limits (see later). However, it has stimulated regular discussion of data privacy issues between governments in the region, and more systematic cooperation between DPAs in the region on cross-border enforcement.

The APEC approach was initially enthusiastically supported by at least the USA, Australia, Canada and Mexico, and acquiesced to by other countries. However it has comprehensively failed to establish an alternative paradigm for data protection: almost no evidence of adoption of its principles in legislation in the region (the one obvious example, still not enacted, is discussed later under ‘Accountability’); no increase in self-regulatory initiatives; and a faltering CBPR initiative (Greenleaf, 2008; Waters, 2008; Waters, 2011). New laws in the region are influenced more by the EU Directive than by the APEC Framework, as discussed throughout this Chapter. APEC’s attempt at establishing a regional form of cross-border privacy rules (CBPR) with national endorsement seems to be on the verge of collapse, crippled by the lack of enforcement mechanisms in some jurisdictions, the opposite problem of stricter legal requirements in others, and a general decline in

interest in involvement by most APEC economies (Waters, 2008, 2011). Attempts are still being made at APEC meetings to finalise governance of the whole scheme. As discussed in the conclusion to this chapter, global analyses of data privacy developments still tend to accord too much significance to the APEC Framework as a brake on European influence. It is more likely that it will be seen as a dead-end: why pay attention to non-binding guidelines that no-one follows?

ECOWAS and other regional agreements on data privacy

The Economic Community of West African States (ECOWAS), a grouping of fifteen states under the Revised Treaty of the ECOWAS, agreed to adopt data privacy laws in 2008, and then adopted a *Supplementary Act on Personal Data Protection within ECOWAS* (ECOWAS, 2010). This supplement to the Treaty establishes the required content of such data privacy laws, influenced very strongly by the EU Directive, and that each state is to establish a data protection authority. As noted earlier, four ECOWAS states have so enacted laws (Benin, Burkina Faso, Cape Verde, and Senegal), and a Bill is before Parliament in Ghana.

ASEAN (the Association of South East Asian Nations) has a much weaker agreement among its eleven members to increase their data privacy protection by 2015 (Connolly, 2008; Munir and Yasin, 2010), but three have legislation in progress (Thailand, the Philippines and Singapore), and one has legislated (Malaysia). In Latin America the four Mercosur countries have agreed to establish Guidelines, but they are not completed (Palazzi, 2011). The prospects for a 'regional bloc' of consistent data protection laws, similar to what has occurred in Europe, seem strongest in West Africa. It is possible though less immediately likely that such developments could also take place in other African sub-regions, South-East Asia or Latin America, although not in the Asia-Pacific as a whole or the APEC sub-set of countries.

CoE Convention 108 and Additional Protocol: A global agreement?

An adequacy finding from the EU does not impose any reciprocal obligations on the recipient country outside the EU to allow free flow of personal data from it to EU countries, but this reciprocal obligation can arise if the non-EU country becomes a party to the Council of Europe data protection Convention (CoE, 1981).

Convention 108 (the *Convention for the protection of individuals with regard to automatic processing of personal data*) Articles 5-8 set out in 'broad brush fashion' a set of data privacy principles that 'were hardly ground-breaking at the time of the Convention's adoption' 30 years ago (Bygrave, 2008). They are even more modest today. However, they did contain versions of almost all the elements we now recognised as core data privacy principles, and are similar to those found in the OECD Guidelines due to cross-influences between the drafters of the two instruments. The 2001 Additional Protocol (ETS 181) to the Convention adds a commitment to data export restrictions, to an independent data protection authority, and to a right of appeal to the courts, and brings the standards of the Convention approximately up to the same level as the Directive (thus showing how the Directive has also influenced other international instruments: Bygrave, 2010). Thirty European countries have also ratified the Additional Protocol (see the Table). Twelve countries that have ratified the Convention (plus three territories on whose behalf the UK acceded to the Convention) have not ratified the Additional Protocol, but in almost all cases that does not matter because they are EU member states, or their laws have been found 'adequate' by the EU, and they have already have the same obligations as the Additional Protocol would impose.

Convention 108 Article 12 always allowed in principle for non-European states to accede to the Convention (and thus to the Additional Protocol as well), by invitation of the Committee of Ministers under the Convention. But the Committee never issued any such invitations, and there was no means of applying. However, in 2008 the Committee explicitly agreed, in effect, that the Consultative Committee under the Convention could receive and assess applications to accede, and it would then consider such applications and issue invitations to accede where appropriate. The

importance of this is that Convention 108 is the only realistic possibility for a global binding international agreement on data protection to emerge. In comparison, the likelihood of a new UN treaty being developed from scratch are miniscule, or as Bygrave puts it, ‘realistically, scant chance’ (2010, p181).

Because it has 42 existing members, there are significant advantages for non-European states to accede to Convention 108 and the Additional Protocol. These fall into three categories. In relation to EU countries, non-European states obtain a guarantee of free flow of personal data from the EU country (unless the EU country derogates from Convention 108 on that point), which the Directive does not give them. While Convention 108 accession will not automatically lead to a finding of ‘adequacy’ by the EU, it is hard to see the EU denying a finding of adequacy to a non-European state that accedes to the Additional Protocol as well as the Convention. Practically, it does not even seem necessary: none of the non-EU European countries that are Council of Europe members (and parties to the Convention) have even bothered applying for an adequacy finding (see the Table). In relation to other non-EU countries that are parties to the Convention, there arise mutual obligations of free flow of personal data between them, unless either derogates because of the other’s lack of a data export restriction. Then there are more general advantages: it is a modest step toward a stronger international data protection regime, not a radical one; it involves voluntary acceptance as an equal party to a treaty of obligations concerning data, rather than by what can be seen as the unilateral imposition of a standard by the EU; and it avoids the necessity for individual countries to make decisions about which other countries have privacy laws which are ‘adequate’ or ‘sufficient’ to allow personal data exports to them. Depending on how long it takes the Committee of Ministers to make decisions, and whether those decisions are perceived to be fair and not unduly political, it could be a more attractive process than applying for an ‘adequacy’ finding to the EU Commission, and sufficient in practice even though not technically a substitute for that. However, it remains to be seen in practice if Convention 108 accession becomes either an alternative to, or a ‘short cut’ to, an adequacy finding for non-European countries. The process might also work in reverse, with the Council of Europe in effect ‘rubber stamping’ requests by non-European states that have received adequacy findings to accede to the Convention and Additional Protocol.

The main disadvantage to non-European countries could be that, if the Committee of Ministers allows countries outside the EU to accede to the Convention with laws of low standard, or without acceding to the Additional Protocol as well, this could result in an obligation (at least on non-EU countries) to allow data exports to countries with sub-standard laws. Only the practice of the Committee can resolve such questions. There is also a lack of mechanisms for citizens of countries outside Europe to enforce the Convention, including their inability to take cases to the European Court of Human Rights. Some of these matters could be dealt with in the current review of the Convention.

There is as yet little of substance to suggest that Convention 108 will become a key instrument of global governance of privacy. However, it has no realistic competitors as a global privacy instrument. Uruguay is apparently the first country to indicate its interest in accession (see CoE 108 accessions, 2011, note under ‘Non-member States of the Council of Europe’). A key factor may be whether members of a regional data privacy agreement such as ECOWAS see Convention 108 accession as a collective means of establishing free flow of personal data between their region and Europe, and other countries. Globalisation of Convention 108 could become one of the most important developments in privacy governance over the next decade, but it is too early to tell.

Data privacy principles

Why we value ‘data privacy’, and how we conceptualise the values that are served by the concept ‘data privacy’, are beyond the scope of this chapter, though of considerable importance, and matters of dispute (see Bygrave 2002, Chs 6-8; 2010, parts 2-4 for an overview, or Bennett and Raab 2006,

Ch 1 for a different approach). Instead, I will analyse the elements of ‘data privacy’ as it has emerged in international agreements and national legislation, and future directions.

Nature and limits of data privacy principles

The closest legal analogy to data privacy principles/rights is copyright. Both are bundles of rights which defy summation in a single phrase, but require precise enumeration of each right that makes up the ‘bundle’ we call ‘copyright’ or ‘data privacy’ in shorthand. We think we know intuitively what ‘copyright’ means, but technically it is a bundle of specific rights (‘adaptation’ ‘reproduction’, etc), which benefit authors (or other copyright owners), and differ between types of works. ‘Data privacy’ doesn’t have a simple definition either, and is similarly a bundle of specific rights (‘access’, ‘limited collection’, ‘security etc), benefitting data subjects in this case, and which can differ between types of personal information. In both cases, enforcement differs between countries, and takes many forms.

The key distinction within data privacy principles is between those principles that do not significantly impede the expansion of data surveillance by organisations but may make them work more fairly (‘efficiency’ principles: Rule and others, 1981) and those that do tend to limit expansions of surveillance (which we can call ‘surveillance limitation principles’). As discussed, the USA has by-and-large limited its controls to the former (including access and correction in some areas, and security generally) and tried to ignore the latter (particularly the collection limitation principle), whereas the EU Directive, and laws influenced by it, include some elements which can be interpreted to impose significant limits on surveillance activities. This distinction is valuable for analysis of the extent to which a data privacy law assists, or impedes, the development (or legitimating) of expanded data surveillance. Another distinction is between principles that ‘empower’ individuals and those that ‘impose obligations’ on data controllers (Bennett and Raab, 2006, pp 121-5). Although not clear-cut, it helps to identify laws which enable individuals to exercise self-help rather than relying on ‘paternalistic’ enforcement (often absent) by DPAs or the state, and also to analyse where responsibility for initiating action lie (with the individual, the data controller, the DPA or the state).

All data privacy laws are based on some variant of a definition of ‘personal data’ or ‘personal information’, meaning that the individual who seeks protection must be identifiable from the information concerned, or from that information and (variously described) other information with which it can reasonably be assumed it may be combined. A range of legislative formulae express this common idea.

This definition of ‘personal data’ imposes two main limitations on the scope of data privacy laws. First, they do not extend to data which does not identify a person but does enable interaction with that person to take place in some way which is ‘personalised’. Sometimes this will involve combining it with other information about the same (non-identified) person. Much new behavioural marketing does not require identification, it only requires increasingly sophisticated interaction. It is arguable whether the full panoply of data privacy principles should apply to all such interactions, or to only a sub-set, such as geo-location data. Second, if personal data is not stored in some material non-transitory form, data privacy principles will usually not apply (New Zealand is an exception, where case law has held that ‘storage in the mind’ suffices). Some forms of CCTV, for example, are therefore excluded. It is also arguable that this is an appropriate dividing line between data privacy laws and surveillance limitation laws.

Core data privacy principles

With data privacy legislation in 75 jurisdictions (plus sub-national laws), it is not surprising that privacy principles are expressed in many differing forms, and that there are some principles which are only found in a few (or even one) piece of legislation. The most influential distinction between ‘core’ and ‘non-core’ principles is that of the Article 29 Working Party’s interpretation of the EU

Directive in order to operationalise the Article 25 ‘adequacy’ criterion (A 29 WP, 1997, 1998). Although their choice has not been contentious, the EU Commission is now proposing to ‘define core EU data privacy elements’ for the purposes of international agreements with the EU and the purposes of adequacy assessment (EU Commission, 2010, 2.4.1).

The language and structure of data privacy principles fall into two main families, plus some hybrids. EU-influenced sets of principles tend to be organised around a broad requirement of ‘fair and lawful processing’, plus various other obligations, whereas laws with a stronger OECD influence (usually outside Europe) tend to avoid the broad ‘fair and lawful processing’ principle, unpacking it at the outset into a number of separate principles (including purpose specification, collection limitation, data quality, and use/disclosure limitation), but also adding others as does the EU. In substance, the result is much the same in what is covered, though not necessarily in the strength of coverage. If we look for the substantially common elements in the EU’s ‘core’ elements and the ‘Principle of National Application’ in the OECD Guidelines, a common core of data privacy principles (expressed here in non-Eurocentric language), can be listed as follows (with some indication of significant variations):

1. *Collection* - limited, lawful and by fair means; generally with consent or knowledge (OECD 7; EU A 6(1)(a)); EU is more specific that collection must be minimum necessary (EU A 6(1)(b), (c))
2. *Data quality* – relevant, accurate, up-to-date (OECD 8; EU A 6(1)(d)); EU adds requirement to de-identify or delete when use complete (EU A6(1)(e))
3. *Purpose specification* at time of collection (OECD 9; EU A6); EU more explicit on legitimacy of purpose (EU A 7)
4. *Notice* of purpose and rights at time of collection (OECD ambiguous; EU A 10, 11)
5. *Uses* (including disclosures) limited to purposes specified or compatible (OECD 10)
6. Reasonable *security* safeguards (OECD 11; EU A 17)
7. *Openness* re personal data practices, including to persons other than data subjects (OECD 12); not specific in EU except in relation to data subjects (EU A 10, 11)
8. Individual rights of *access and correction* (OECD 13; EU A 12); EU adds right to object (EU A 14)
9. Data controllers *accountable* for implementation (OECD 14; EU A 6(2))
10. *Data export restrictions* (OECD says they may, but EU says they must, be limited to (a) countries which do not substantially observe these basic rules, and (b) do not prevent circumvention by re-exports) (OECD 17; EU A 25,26)

The Article 29 Working Party’s requirements for adequacy also adds what it considers to be core Principles for specific types of processing including (i) additional safeguards for processing of sensitive data; (ii) a right to opt-out of direct marketing involving use of personal data; (iii) additional safeguards for automated processing of personal data; and (iv) special care in the operation of identifiers of general application (like national ID numbers or cards).

Data export limitations and ‘adequacy’

There are two main means by which countries can attempt to have their standards for data privacy continue to apply to information about their citizens or residents (or even those whose data has been processed on their territories): (i) give their own laws extra-territorial application under some

circumstances; and (ii) impose limitations on when personal data can be exported from their country to other countries.

Concerning extra-territorial application (the ‘applicable laws’ question) the aim of the EU Commission is to ‘ultimately provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller’, through reforms to provisions concerning applicable law (EU Commission, 2010, 2.2.3). While their principal goal is to ensure that only one law applies within the EU internal market (and that it is clear which one applies), they also intend to apply this to ‘data controllers established outside’ the EU or the EEA. Jurisdictions outside Europe are equally enthusiastic about giving their data privacy laws extra-territorial effect, as can be seen in the laws of Australia, Hong Kong and India. There will inevitably be political and legal conflicts of considerable significance over this question of ‘applicable laws’.

Concerning the second approach, data export limitations, the EU’s ‘border control’ approach is to limit data exports unless ‘adequate protection’ can be demonstrated at the receiving end (EU Directive Articles 25, 26). In summary ‘[t]he effect of a Commission adequacy finding is that personal data can freely flow from the 27 EU Member States and the three EEA member countries to that third country without any further safeguard being necessary. However, the exact requirements for recognition of adequacy by the Commission are currently not specified in satisfactory detail in the Data Protection Directive’. There is a further problem that different EU Member States make different judgments on adequacy (EU Commission, 2010, 2.4.1).

As yet, the EU has only made ‘adequacy’ decisions in relation to nine jurisdictions as a whole (Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, and Jersey), a minority of which are of economic or political significance. Uruguay and New Zealand will soon be added to this list, following positive findings by the increasingly pragmatic A 29 Working Party (Greenleaf and Bygrave 2011). It is arguable that Colombia, Mexico and Peru also have adequate laws (Palazzi, 2011), South Korea and India could each put forward a case after their 2011 reforms, as could Taiwan (with more difficulty), and Hong Kong and Australia might do so after their legislatures complete their reform processes (see generally Greenleaf, 2011a). The new laws in Africa resemble the EU Directive in their principles, so arguments for adequacy would hinge largely on issues of effective enforcement. For European countries that have acceded to both Convention 108 and the Additional Protocol, an adequacy finding is not needed. But there could be significantly more adequacy findings outside Europe if the EU was more pro-active.

Despite the tardiness of the EU in making assessments, the desire to eventually obtain an ‘adequacy’ finding from the EU, or in a more amorphous form, to have one’s law regarded as of the highest international standard (that the EU Directive is considered by many to embody) has been a significant influence on the development of laws outside Europe (as discussed above). The EU has been unwilling to make, and publicise, a sufficient number of decisions about what does and does not constitute adequate protection. Nor do European countries seem to have blocked particular data exports as frequently as occurred during the 1980s and 1990s, further reducing the impact of the adequacy requirement. Bygrave (2010, p 197) asserts there is considerable inconsistency and non-enforcement by EU members in relation to the data export provisions.

Outside Europe, ‘border control’ data export limitations are found in the majority of data privacy laws, and are sometimes added when there are revisions of existing laws. Various such limitations can now be found in the legislation of Australia, New Zealand, Taiwan, South Korea, India, and Macau, though their strength varies a great deal. There are provisions not yet in force in the laws of Malaysia and Hong Kong. Such restrictions already exist in the data privacy laws of the Latin American countries (except Chile), and the African countries.

The contested principle of ‘accountability’

Providing an alternative to the ‘border control’ approach is one objective of some proponents of the so-called ‘accountability’ principle, though they do not usually present it this way. Whether an ‘accountability’ principle strengthens or weakens data privacy depends very much on what you mean by ‘accountability’, because the term is ill-defined and fluid in the literature supporting it, which some of its proponents admit (Alhadef, Van Alsenoy and Dumortier, 2011).

The OECD Guidelines have an Accountability Principle (principle 14) but all it says is that a data controller ‘should be accountable for complying with measures which give effect to the [other] principles’, and the EU Directive has a similarly uncontentious provision (A 6(2)). The Article 29 Working Party’s ‘Accountability Opinion’ of (A 29 WP, 2010) proposes ‘a statutory accountability principle’ which would add a new enforceable principle requiring data controllers to put effective measures into place to comply with other principles, ‘and demonstrate this on request’. It suggests complementary specific requirements like PIAs ‘for higher risk data processing’. Although the European Commission (EU, 2010) says it will ‘take account of the current debate on the possible introduction of an ‘accountability’ principle’, all it has as yet proposed under that heading are three improved methods of enforcement (discussed later): mandatory DPOs, mandatory DPIAs/PIAs in some situations; and promotion of PETs and ‘privacy by design’. ‘Accountability’ should also not be confused with more precise notions of ‘binding corporate rules’ (BCRs) as a means of allowing data exports. The BCR approach of the A29 Working party opinion on BCRs (A29 WP, 2003) is all about exactly how legal liability is guaranteed in BCRs, and particularly ‘third party beneficiary rights’. Here, ‘accountability’ has a strict meaning of ‘legal liability’. None of these developments are objectionable.

The problem arises when proponents of ‘accountability’ present its elements without defining precisely what is their relationship to legal liability for breaches of privacy principles, by whom, and with what standards of proof. Abrams (2011), a leader of the ‘Accountability Project’, describes the ‘two pieces to accountability’ as a ‘compliance program’ and ‘demonstration capacity’, but without any reference to their relationship to legal liability, either to the regulator or data subject. Alhadef and others, while stating that ‘accountability’ is not a substitute for ‘adequacy’, want it to count toward an assessment of adequacy in a way that remains undefined (Alhadef, Van Alsenoy and Dumortier, 2010, p25). Later, they refer to the possibility of ‘accountability mechanisms’ becoming ‘a credible alternative to the existing mechanisms for international transfer’ (p 26), which seems to contradict their previous denial. This ambiguity is latent in the APEC Privacy Framework, which is completely silent on data export restrictions. Thus the APEC Accountability Principle (IX) becomes the only principle under which any liability for data exports could arise. All it says in clarifying that a data controller ‘should be accountable’ is that it should ‘exercise due diligence and take reasonable steps to ensure’ that overseas recipients ‘will protect the information consistently with these Principles’. This APEC principle is translated in a Bill still before Australia’s Parliament into a principle which allows exports of personal data to any country in the world, with the onus remaining on the data subject to prove that breaches of data privacy principles by the recipient occurred there, before the exporter suffers any ‘accountability’ at all. Gathering such proof would be a dangerous and expensive activity in many countries (Greenleaf, 2010). The danger that ‘accountability’ is a Trojan horse for the replacement of data export restrictions based on ‘border control’ with a pseudo-restriction that is in practice meaningless is the reason that it requires this lengthy discussion. A satisfactory solution to the problem of data exports may be elusive, but ‘accountability’ is not it.

In a survey of the data protection accountability literature, Raab (2011) – neither proponent nor opponent – finds ‘little help’ in answering the crucial question posed by Bennett (2010), ‘accountability for what and to whom’, when it comes to defining the relationships between the bodies who are supposed to be involved in delivering accountability (‘accounting firms, standards bodies, seal and trustmark programs [and] mediation and dispute resolution bodies’: Bennett, 2010),

and ‘the public whom they ultimately protect’. He is also particularly concerned that the Accountability Project suggests that some of its ‘nine fundamentals’ can be ‘customised’ (reduced) in particular, without explaining what ‘accountability’ will attach to the making of this decision. ‘Accountability’ is not gaining a precise meaning despite years of discussion, and should not play any significant role in data privacy beyond its possible value in making data processors legally liable for carrying out specific activities to implement data privacy principles, rather than just hoping that they will not be caught breaching them. It should not reduce or substitute for any other obligations.

Emergent data privacy principles

The EU Commission is considering proposing the introduction of five new or expanded principles (EU Commission, 2010, 2.1):

- *Transparency* – ‘a general principle of transparent processing of personal data’, including ‘specific obligations for data controllers on the type of information to be provided’, and ‘one or more EU standard forms (‘privacy information notices’) to be used by data controllers’;
- *Data breach notification* – ‘a general personal data breach notification, including the addressees of such notifications and the criteria for triggering the obligation to notify’, to apply when personal data is ‘accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons’ is to be mandatory;
- *Improved means to exercise rights* – ‘improving the modalities for the actual exercise of the rights of access, rectification, erasure or blocking of data’ by deadlines, electronic exercise and access free of charge;
- *‘Right to be forgotten’* – ‘the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes’, though perhaps only a clarification of the existing principle concerning deletion, is likely to be of particular importance in relation to social networks and the organisations with access to social network data for data mining.
- *‘Data portability’* – ‘providing the explicit right for an individual to withdraw his/her own data (e.g., his/her photos or a list of friends) from an application or service so that the withdrawn data can be transferred into another application or service, as far as technically feasible, without hindrance from the data controllers’, is likely to be of seismic importance to the providers of social network services, who will be given an incentive to compete on data privacy as well as on other grounds. At present their services are not interoperable (it is not possible to have ‘friends’ etc on a different service), and while this proposal does not go as far as that, it would allow users to migrate in bulk to other services, taking all their personal data (User Generated Content) with them (provided the ‘right to be forgotten’ is also implemented).

The Commission is also considering other expanded rights including ‘clarifying and strengthening the rules on consent’ and may expand the categories of data to be considered as ‘sensitive data’, for example genetic data.

Outside Europe, many of these emergent international data privacy norms have already started to be incorporated in laws or legislative proposals. The USA has to some extent led the way with the development of data breach notification rights, but these are also now incorporated in the data privacy laws of Taiwan and South Korea (Greenleaf, 2011a, 2011e), and in proposed legislation in Australia (Greenleaf and Waters, 2010). South Korea also has an explicit ‘no disadvantage in case of refusal’ rule, requiring provision of services, with no extra costs, where data privacy rights are exercised. Australia has since 2001 had a specific principle requiring the option of anonymous

transactions wherever this is feasible, whereas the EU's proposals for stronger data minimisation are not this explicit. Genetic data is already explicitly included in India's new law. Because of innovations like these at the national level in APEC economies, the EU Commission's proposals are unlikely to increase divergence in data privacy standards around the world in the long term. If they widen the gap between EU and APEC principles, that will only make APEC more irrelevant.

Data privacy enforcement

In addition to privacy principles, the other requirement for a data privacy law is that it provides a means of enforcing them by law. In practice, as we have seen, almost all data privacy laws provide for an independent authority (a DPA) to be involved in their enforcement. But after that the common elements are more difficult to identify. And just because there are rising standards of data privacy principles, it does not necessarily follow that there will be a concomitant rise in levels of enforcement (Bennett and Raab, 2006).

There are of course many other roles of a DPA that contribute to the governance of privacy, including their roles in influencing legislation, government policies, and business practices to develop in ways which are less privacy invasive. These are not the focus of this chapter but are analysed by Bennett and Raab (2006, pp 133-43)) as involving roles as ombudsmen, auditors, consultants, educators, policy advisors, and negotiators. However, they correctly state, their central role is as enforcers and the key question is the powers they have to order compliance with privacy principles (p 143). It is more complex, because only some DPAs have an 'original jurisdiction' empowering them to make enforcement orders when they reach conclusions, rather than referring the matter to a court or tribunal for enforceable orders. In any event, there is almost always a right of appeal from a DPA's decisions to a court or tribunal (one exception is that the complainant has no appeal in Australia from a determination by the federal Privacy Commissioner: Waters and Greenleaf, 2010).

Standards for enforcement mechanisms

There is no internationally accepted standard of what constitutes appropriate or sufficient enforcement of a data privacy regime. As with principles, the most widely accepted standard is the Article 29 Working Party's interpretation of what types of enforcement mechanisms and levels of effectiveness constitute 'adequate' enforcement in relation to the EU Directive (A29 WP, 1997, 1998). These are (with quotations from the 1998 Opinion):

- (i) Delivery of a "good level of compliance" with the content rules (data protection principles): 'A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important [role] in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.'
- (ii) Provision of support and help to individual data subjects in the exercise of their rights: 'The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.'
- (iii) Provision of appropriate redress to the injured party where rules are not complied with: 'This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.'

Other international agreements have contributed little. The OECD Guidelines recommended legislation, but not a DPA, and the CoE Convention did not require a DPA until the Additional Protocol. The APEC Framework's approach to enforcement was completely non-prescriptive, allowing any method of enforcement (Greenleaf, 2010), and this may be one of the reasons for its failure to date. Various APEC members have enacted laws which have enforcement mechanisms meeting EU standards, in some cases tailored to meet local needs (eg Korea's unique mediation system: Greenleaf 2011a).

The one other area in which separate international standards have emerged is for the independence of DPAs as a condition for their membership of international associations of DPAs (IDPPC, 2001) but details are beyond the scope of this Chapter. Most DPAs established by data privacy laws meet these standards (the Macao authority can only be an observer at meetings because its enabling law has not yet been passed). The Malaysian DPA (not yet appointed) is likely to be an example of where the data privacy legislation fails to provide sufficient independence (it makes the DPA subject to Ministerial direction), and is likely to result in accreditation being refused (Greenleaf, 2010e; Munir and Yasin, 2010). The European Commission has also taken action against Germany because of the lack of independence of some of its regional DPAs.

The poor enforcement record of most DPAs

It is not possible here to analyse the enforcement record of what are now nearly 70 DPAs, some of whose activities go back decades. There are no accepted evaluation criteria for the effectiveness of data privacy regimes as a whole (Bennett and Raab, 2006, p235), and nor are there for assessing the overall effectiveness of DPAs. However, they rarely win accolades for effective enforcement. In Europe the EU Commission admits that '[t]here is consensus among stakeholders that the role of Data Protection Authorities needs to be strengthened so as to ensure better enforcement of data privacy rules' (EU Commission, 2010, 1). There are a string of European studies since 2003 (summarised by Bygrave, 2010, p197) documenting under-resourcing of enforcement efforts by DPAs, patchy compliance by data controllers (although they are generally supportive of data privacy objectives), and low awareness of data protection rights by individuals. Outside Europe, there is little evidence of a better enforcement record. In Asia and Australasia my own studies of Japan, Hong Kong and Australia give details of poor enforcement in those countries, due to a combination of inadequate enforcement powers (particularly Hong Kong and Japan), lack of appeal rights (Australia and Japan), and unwillingness to use those powers that are available (everywhere) (Greenleaf, 2010a, 2010b, 2010c). The only DPA which is considered to enforce its legislation effectively is New Zealand (now endorsed by the A 29 Working Party finding of adequacy), with South Korea's enforcement having some credibility in the private sector but none in the public sector (Greenleaf, 2011a provides a summary).

One near-universal contributor to the poor compliance record of DPAs is their failure to sufficiently document what they do about resolving complaints. There is a general under-reporting by DPAs of both the legal aspects of complaint resolutions and the outcomes of investigations. This results in a failure of 'responsive regulation' because of the lack of feedback loops concerning 'the tariff' that can be expected by complainants and respondents alike in relation to particular types of breaches (Greenleaf 2004a). Lack of objective standards of what will/must be reported (both case examples and statistics) is a failure of accountability. It is one that has as yet been neglected by the European Commission, and by most DPAs whether European or not. However, the world's DPA have recently resolved to report summaries of selected complaints, in a more consistent form, and to help make case law in their jurisdictions more readily findable. (ICDPPC, 2009).

Emergent mechanisms for enforcement

New enforcement mechanisms are developing as standard tools of DPAs, but less coherently than emergent Principles. In Europe, the EU Commission proposes, in light of its finding of the need to

provide better enforcement, the following strengthening of European enforcement mechanisms (EU Commission, 2010, 2.2.4-5):

- *Representative actions* – ‘extending the power to bring an action before the national courts to data privacy authorities and to civil society associations, as well as to other associations representing data subjects' interests’;
- *Stronger sanctions* – ‘for example by explicitly including criminal sanctions in case of serious data protection violations’;
- *Mandatory independent Data Protection Officers* – with harmonised rules related to DPO’s tasks and competences;
- *Data protection impact assessment* – to be an obligation of DPOs in defined situations ‘when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance’.

Some EU Commission proposals are more in the nature of intended activities rather than new legal requirements, such as ‘further promoting the use of PETs [privacy enhancing technologies] and the possibilities for the concrete implementation of the concept of ‘privacy by design’ and ‘the possible creation of EU certification schemes (e.g. ‘privacy seals’) for ‘privacy-compliant’ processes, technologies, products and services’.

Most of these proposed improvements are also found in at least some jurisdictions outside Europe. For example: representative actions are already provided for in Australia, Korea, Taiwan and (arguably) Hong Kong; collective mediation proceedings are a novel element in Korea; criminal sanctions for serious breaches of principles are included in pending Bills in Hong Kong and Australia; and Privacy Impact Assessments (PIAs) are already mandatory in some circumstances for the public sectors in the US, UK and Canadian federal governments and will be in the Korean public sector. There is already a good deal of ‘trading up’ of remedies between jurisdictions in the Asia-Pacific, quite apart from influences from Europe.

New challenges of a networked world: Can data privacy laws cope?

All the new technological challenges noted at the outset of this chapter are interconnected and multiply the effects and dangers of other changes. Take, for example, more ubiquitous data collection: ‘The ubiquity of personal data and of data gathering means that the default position is shifting from state and private bodies having to decide to collect data to one in which they have to make an effort not to collect (increasingly sensitive) data’ (Korff, Brown et al, 2010). Where this occurs, then the privacy dangers of social networking services (SNS), or data mining, are multiplied accordingly.

The fact that the location of such a large proportion of Internet services posing the most significant privacy threats (search engines, SNS etc) is in the USA makes American exceptionalism in data privacy far more significant than it would otherwise be. When that is coupled with the ease with which ‘cloud computing’ makes it technically possible for data to be transferred between servers and service providers (eg call centres) located in successive countries within a single day, the problem of data controllers being ‘out of reach’ of regulators concerned with protection of citizens of particular countries is clearly getting worse.

Under such circumstances, is it realistic to think that data privacy laws have any prospect of providing privacy protection? It is probably true that current laws (and enforcement practices) cannot and do not cope very well. But that is not the end of the matter, given the considerable strengthening of data protection laws proposed by the European Commission, and the legislative changes already taking place in the United States and in countries outside Europe. Perhaps one way of answering the question is to assess what are the main dangers posed by various new

technologies, followed by assessing whether any of the proposed legal changes address those problems. So this chapter concludes with two examples of such juxtaposition, SNS and cloud computing.

Example 1: Social networking services (SNS)

	Danger to privacy	Proposed reform
1	Default settings are anti-privacy	Mandatory defaults
2	Users don't know how to control privacy settings	Mandatory default re-sets
3	Data mining for marketing purposes	'Do not track' Principle or explicit disclosures
4	3rd parties add personal data (photos etc) without permission	Simpler confidentiality / privacy actions between SNS users; Take downs' by SNS operators would also assist.
5	Tagging is out of user control	'No tagging' in 'Do not track'
6	Personal data can't be removed from SNS	'Right to be forgotten'
7	Non-interoperability of SNSs	Data portability' but cannot mandate interoperability?
8	Facebook dominance reduces incentive for better privacy policies	More competition, such as Google+

Example 2: Cloud computing

	Danger to privacy	Proposed reform
1	Data users lose control of physical location of data (Data can go to locations with no privacy controls)	Data export laws based on physical destination; also improved notice
2	Other jurisdictions can impose legal control (eg USA Patriot Act can apply)	No answer once physical control lost
3	Individuals have no idea where their data is located	Disclosure of export locations; Can also require consent
4	Security failures of cloud service providers (eg DropBox 4 hours with no passwords on accounts)	Vicarious liability of local data user

The reader is invited to consider whether future data privacy laws may be able to cope with new technical and social developments such as these. It is arguable that data privacy laws are in a period of creative re-development, within Europe and elsewhere, including the USA, and that they may cope better in future than they are capable of at present. In addition, whatever their shortcomings, they are still the best regulatory response that we have, so we should use them.

Conclusion – The trajectory of global data privacy regulation

Bennett and Raab (2006), in the most systematic global review of data privacy regulation, presented their 'main research question' (p xv) as whether there was a 'race to the bottom', a 'race to the top', or something else, in the global development of data privacy protection. They correctly caution that the existence and formal strength of a data privacy law is only one factor by which we should measure data privacy protection in a country, and two other key dimensions are the effectiveness of enforcement and the extent of surveillance (discussed below). Therefore, globally, there is more than one race to the top or bottom.

They noted that, in relation to legislation, the main conditions proposed by globalisation theories of regulation for a 'race to the bottom' (data mobility and wide national divergences in laws) were present in the case of data protection legislation (p276). Nevertheless, they found that 'there is clearly no race to the bottom', but nor did they find clear evidence of a 'race to the top', or global ratcheting up of privacy standards. In particular, they considered that the 'general suspicion that the APEC Privacy Principles are intended as an alternative, and a weaker, global standard than the EU' means that they 'may serve to slow and even reverse' the otherwise 'halting and meandering walk' to higher standards which the EU Directive had inspired (p283). They concluded that the most

plausible future scenario (the Bennett-Raab thesis) was ‘an incoherent and fragmented patchwork’, ‘a more chaotic future of periodic and unpredictable victories for the privacy value’ (p295). So Bennett and Raab found some ‘upward’ global trajectory influenced significantly by the EU Directive, but sufficiently weak in the mid-2000s that the countervailing weakness of the APEC approach was enough to make the future quite unpredictable.

Half a decade later, it can be argued that there is now a clearer ‘upward’ global trajectory than Bennett and Raab found, provided we keep clear that we are only talking about the existence and formal strength of data privacy laws, not the other factors. Their analysis is based on the existence of only ten data privacy laws (on my definition) in countries outside Europe, plus two covering only the public sector. That was probably an under-estimate in 2006 because of some little-known laws, but in any event by mid-2011 there are 27 data privacy laws outside Europe (as many as there are EU member states), and a handful of Bills expected to be enacted soon. Surprisingly, Bygrave’s more recent global analysis of data privacy developments only assumes that ‘well over 40 countries’ have data privacy laws, (Bygrave, 2010, p166), even though he is aware of the new African laws in francophone countries (p 193). This reflects the previous lack of availability of a catalog showing that there are now more than 70 such laws. As argued above, the rate of expansion is greater than ever before. Of course, the number of data privacy laws can only be part of the measure, but in Africa, Latin America and even in Asia the European Directive has become the single most significant influence on the content of those laws, and leads to them embodying a relatively high standard of data protection principles. The lower standards of the APEC Privacy Framework have not served to ‘slow or even reverse’ this trend as Bennett and Raab and others (myself included) feared.

A handful of new data privacy laws across the globe each year, with EU-influenced privacy principles, and revisions of some existing weaker laws to strengthen them, does not constitute a ‘race’ in most uses of the term, but nor does it any longer look like such a ‘halting and meandering walk’ as Bennett and Raab found. It may not be a race, but data privacy laws do have a global trajectory, namely expansion at an increasing rate with principles more commonly influenced by the EU Directive than any other source.

Furthermore, the EU’s own standards show every likelihood of strengthening, as do data privacy standards originating outside the EU. The global ‘ratcheting up’ of standards is likely to continue, at least in the near future. It is not possible to predict whether the Council of Europe Convention 108 and Additional Protocol will develop toward a global privacy agreement but if they do this will help accelerate global expansion (though perhaps not the strength of standards). The influence of some ‘accountability’ advocates (coupled with unchecked growth in ‘cloud computing’) is more likely to be a future countervailing factor than the APEC Privacy Framework.

As mentioned, Bennett and Raab counsel against any one-dimensional measure of data privacy laws, and their cautions must be heeded, though they are largely beyond the scope of this chapter. First, a strengthening of privacy standards (principles) does not in any way entail a corresponding increase in the enforcement of those standards (or its effectiveness). As discussed earlier, weak enforcement is a global problem for data privacy laws, and although there are valuable new enforcement mechanisms being developed, it is a separate question in every jurisdiction whether enforcement is improving. Second, there is no necessary correspondence between a rise in data privacy standards and a decrease in surveillance practices. In fact, in some countries the enactment or strengthening of privacy standards has been an explicit ‘trade off’ for new surveillance practices authorised or mandated by legislation. As Bennett and Raab conclude, there is not one race to the top or bottom that we must consider. It is better to say that the various dimensions on which we must measure the health of privacy as a value, including data privacy principles, their enforcement, and surveillance practices. These dimensions, as they say, differ from place to place and time to time, and are not readily ‘balanced’ into one overall measure. Nevertheless, considered solely on

the dimension of the global spread of EU-like data privacy laws, the Bennett-Raab thesis no longer appears correct. On the other dimensions of effective enforcement and limiting surveillance, there are no obvious global trajectories which could give rise to similar optimism.

Appendix: Global Table of data privacy laws

This table lists known data privacy laws (as defined above) as at 30 July 2011.

Jurisdiction	Key Act	From ¹	Latest	Region	EU ²	CoE ³	Other Int. ⁴
Albania	Act on the Protection of Personal Data	1999	1999	Europe	[I]	M; P	
Andorra	Law on the protection of personal data	2003	2003	Europe	A	M; P	
Argentina	Personal Data Protection Act	2000	2000	Latin Am	A		
Australia	Privacy Act 1988	2001	2001	Australasia			APEC; OECD
Austria	Datenschutzgesetz	1978	2009	Europe	M	M; P	OECD
Azerbaijan	Law on data, data processing and data protection	1998	1998	Europe		M	
Bahamas	Data Protection Act	2003	2003	Caribbean			
Belgium	Law on Privacy Protection in relation to the Processing of Personal Data	1992	1998	Europe	M	M	OECD
Benin	Loi sur la Protection des données personnelles	2009	2009	Africa			ECOWAS
Bosnia & Herzegovina	Law on the protection of personal data	2001	2001	Europe	[I]	M; P	
Bulgaria	Law for Protection of Personal Data	2002	2007	Europe	M	M; P	
Burkina Faso	Law on Protection of Personal Information	2004	2004	Africa			ECOWAS
Canada	Personal Information Protection and Electronic Documents Act	2002	2002	North Am	A		APEC; OECD
Cape Verde	Loi N° 133/V/2201 du 22 janvier 2001	2001	2001	Africa			ECOWAS
Chile	Privacy Law	1999	1999	Latin Am			APEC; OECD
Colombia	Data Protection Law	2008	2008	Latin Am			
Croatia	Act on Personal Data Protection	2003	2003	Europe	[I]	M; P	
Cyprus	The Processing of Personal Data (Protection of the Individual) Law	2001	2003	Europe	M	M; P	
Czech Republic	Personal Data Protection Act	1992	2000	Europe	M	M; P	OECD
Denmark	Act on Processing of Personal Data	1978	2000	Europe	M	M	OECD
Estonia	Data Protection Act	2003	2003	Europe	M	M; P	OECD
Faroe Islands	Act on processing of personal data	2010	2010	Europe	A		
Finland	Personal Data Act	1987	1999	Europe	M	M	OECD

¹ **Date columns:** ‘From’ = date original law enacted; ‘Latest’ = year of last significant amendment known

² **European Union column:** M = country is an EU member state; A = country’s protection of personal data has been held ‘adequate’ by the EU; [A] = Favourable Article 29 Working Party opinion on adequacy, but no final decision announced; EEA = country is a member of the European Economic Area; [I] = Adequacy finding is in practice irrelevant due to country acceding to both Council of Europe Convention 108 and Additional Protocol

³ **Council of Europe column:** M = country is a member state of the Council of Europe and has ratified the Convention; M* = United Kingdom has ratified Convention on behalf of sub-jurisdiction; P = country has also ratified the optional protocol; S = country has signed but not ratified Convention

⁴ **Other international commitments column:** APEC = ‘economy’ is a member of APEC; OECD = country is a member of OECD; ECOWAS = country is a member of Economic Community of West African States

France	Law relating to the protection of individuals against the processing of personal data	1978	2004	Europe	M	M; P	OECD
FYROM (Macedonia)	Law on Personal Data Protection	2005	2005	Europe	[I]	M; P	
Germany	Federal Data Protection Act	1977	2001	Europe	M	M; P	OECD
Gibraltar	Data Protection Act	2004	2004	Europe			
Greece	Law on the Protection of individuals with regard to the processing of personal data	1997	1997	Europe	M	M	OECD
Guernsey	Data Protection (Bailiwick of Guernsey) Law	1986	2001	Europe	A	M*	
Hong Kong SAR	Personal Data (Privacy) Ordinance	1995	1995	Asia			APEC
Hungary	Law on the protection of personal data and the disclosure of public information	1992	1992	Europe	M	M; P	OECD
Iceland	Law on the Protection and Processing of Personal Data	1989	2000	Europe	EEA	M	OECD
India	Rules under s43A (2008 Amendt), Information Technology Act 2000	2011	2011	Asia			
Ireland	Data Protection Act	1988	2003	Europe	M	M; P	OECD
Isle of Man	Data Protection Act	1986	2002	Europe	A	M*	
Israel	Privacy Protection Act 1981	1981	1981	M.East/N.Af	A		OECD
Italy	Consolidation Act regarding the Protection of Personal Data	1996	2003	Europe	M	M	OECD
Japan	Act on the Protection of Personal Information	2003	2003	Asia			APEC; OECD
Jersey	Data Protection (Jersey) Law	1987	2005	Europe	A	M*	
Kyrgyz Republic	Law on Personal Data	2008	2008	Central Asia			
Latvia	Law on Protection of Personal Data of Natural Persons	2000	2002	Europe	M	M; P	
Liechtenstein	Gesetz über die Abänderung des Datenschutzgesetzes (2002)	2002	2008	Europe	EEA	M; P	
Lithuania	Law on Legal Protection of Personal Data	1996	2003	Europe	M	M; P	
Luxembourg	Data Protection Law	1979	2002	Europe	M	M; P	OECD
Macao SAR	Personal Data Protection Act	2007	2007	Asia			
Malaysia	Personal Data Protection Act	2010	2010	Asia			APEC
Malta	Data Protection Act	2001	2001	Europe	M	M	
Mauritius	Data Protection Act	2004	2004	Africa			
Mexico	Federal Law on the Protection of Personal Data Held by Private Parties	2010	2010	Latin Am			APEC; OECD
Moldova	Law on Personal Data Protection	2007	2007	Europe	[I]	M; P	
Monaco	Act controlling personal data processing (2001)	1993	1993	Europe	[I]	M; P	
Montenegro	Law on Personal Data Protection	2008	2008	Europe			
Morocco	Data Protection Act	2009	2009	M.East/N.Af			
Netherlands	Personal Data Protection Act	1988	2000	Europe	M	M; P	OECD
New Zealand	Privacy Act 1993	1993	2010	Australasia	[A]		APEC; OECD
Norway	Personal Data Act	1978	2000	Europe	EEA	M	OECD
Peru	Law on Protection of Personal Data	2011	2011	Latin Am			APEC; US FTA
Poland	Act on the Protection of Personal Data	1997	2004	Europe	M	M; P	OECD

Portugal	Lei da protecção de dados pessoais	1991	1998	Europe	M	M; P	OECD
Romania	Law on the protection of individuals with regard to the processing of personal data and the free movement of such data	2001	2005	Europe	M	M; P	
Russia	Federal Law Regarding Personal Data	2011	2011	Europe	S	M	APEC
San Marino	Law regulating the Computerized Collection of Personal Data	1983	1995	Europe			
Senegal	Act on the Protection of Personal Data	2007	2007	Africa			ECOWAS
Serbia	Law on Personal/ Data Protection	2008	2008	Europe	[I]	M; P	
Slovakia	Act on the Protection of Personal Data	1992	2005	Europe	M	M; P	OECD
Slovenia	Personal Data Protection Act	1999	2004	Europe	M	M	OECD
South Korea	Data Protection Act	2001	2011	Asia			APEC; OECD
Spain	Ley Orgánica de Protección de Datos de Carácter Personal	1992	1999	Europe	M	M; P	OECD
Sweden	Personal Data Act	1973	1998	Europe	M	M; P	OECD
Switzerland	Data Protection Act	1992	1992	Europe	A	M; P	OECD
Taiwan	Personal Data Protection Act	1995	2010	Asia			APEC
Tunisia	Law on the protection of personal data	2004	2004	N.Af/M.East			
Ukraine	Law on Personal Data Protection	2011	2011	Europe	[I]	M; P	
United Kingdom	Data Protection Act 1998	1984	1998	Europe	M	M	OECD
Uruguay	Law on the Protection of Personal Data	2008	2008	Latin Am	[A]		

References

- A29 WP (2010) Article 29 Data Protection Working Party – ‘Opinion 3/2010 on the principle of accountability’ (WP 173, DG XV, 00062/10/EN, adopted on 13 July 2010)
- A29 WP (2003) Article 29 Data Protection Working Party – ‘Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers’ (WP 74, DG XV, 11639/02/EN WP 74, adopted on 3 June 2003)
- A29 WP (1998) Article 29 Data Protection Working Party ‘Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive’ (WP 12, DG XV D/5025/98, adopted on 24 July 1998)
- A29 WP (1997) Article 29 Data Protection Working Party ‘First orientation on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy’ (WP 4, DG XV D/5020/97-EN final, adopted on 26 June 1997)
- Abrams, M (2011) ‘Accountability 2011’, Powerpoint presentation to *Privacy Laws & Business Annual Conference*, St Johns College, Cambridge, July 2011
- APEC (Asia Pacific Economic Cooperation) (2005) *APEC Privacy Framework*, http://publications.apec.org/publication-detail.php?pub_id=390, accessed 2 September 2011
- Alhadeff, J, Van Alsenoy, B and Dumortier, J (2011) ‘The accountability principle in data protection regulation: origin, development and future directions’, 2011, available at <https://lirias.kuleuven.be/bitstream/123456789/311284/1/Demystifying_accountability_JHA_BVA_JD_final_draft.doc>
- Bennett, C (2010) ‘International privacy standards: Can accountability ever be adequate?’ *Privacy Laws & Business International Newsletter*, Issue 106, August 2010, pp 21-3
- Bennett, C and Raab, C (2006), *The governance of privacy: Policy instruments in global perspective*, Boston, MA: MIT Press.
- Bygrave, L (2010) ‘Privacy and Data Protection in an International Perspective’, *Scandinavian Studies in Law*, 56, 165–200; <http://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/>, accessed 2 September 2011
- Bygrave, L (2008), ‘International Agreements to Protect Personal Data’, in James B. Rule and Graham Greenleaf (eds), *Global Privacy Protection: The First Generation*, Cheltenham, UK and Northampton, MA, US: Edward Elgar, pp. 15–49.
- Bygrave, L (2002), *Data Protection Laws: Approaching Their Rationale, Logic and Limits*, The Hague: Kluwer Law International.
- Bygrave, L (1998) ‘Data Protection Pursuant to the Right to Privacy in Human Rights Treaties’, *International Journal of Law and Information Technology*, 6(3), 247–284.
- Connolly, C (2008) ‘A new regional approach to privacy in ASEAN’, Galexia website, http://www.galexia.com/public/research/articles/research_articles-art55.html, accessed 2 September 2011

CoE (1981) Council of Europe *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

CoE 108 accessions (2011) Council of Europe CETS No.: 108 webpage for accessions and ratifications,

<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG>, accessed 2 September 2011

EU Commission, 2010 'A comprehensive approach on personal data protection in the European Union' (Communication From The Commission To The European Parliament, The Council, The Economic And Social Committee And The Committee Of The Regions), December 2010

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.*)

ECOWAS (2011) Economic Community of West African States (ECOWAS) Press Release 'ECOWAS reaffirms commitment to democracy', 12 August 2011, on ECOWAS website

ECOWAS (2010) Economic Community of West African States (ECOWAS) *Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS* (February 16, 2010)

Greenleaf, G (2011) 'Global data privacy laws: Forty years of acceleration' in (2011) 112 *Privacy Laws & Business International Report*

Greenleaf, G (2011a) 'Asia-Pacific data privacy: 2011, year of revolution?' in *Kyung Hee Law Journal* (forthcoming), available as [2011] UNSWLRS 29 at <<http://law.bepress.com/unswwps/flrps11/art30/>>

Greenleaf, G (2011b) 'India attempts data protection by regulations' *Privacy Laws & Business International Report*, Issue 110, April 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 (2011d) 'The Illusion of Personal Data Protection in Indian Law' (2011) 1 (1): 47-69 *International Data Privacy Law*, Oxford University Press, <http://idpl.oxfordjournals.org/content/1/1/47.full>, accessed 2 September 2011

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

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

Greenleaf, G (2010a) '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, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_count_ry_report_B3_hong_kong.pdf, accessed 2 September 2011

Greenleaf, G (2010b) '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,

http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_count_ry_report_B5_japan.pdf, accessed 2 September 2011

Greenleaf, G (2010c) '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, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_count_ry_report_B2_australia.pdf, accessed 2 September 2011

Greenleaf, G (2010d) '[Australia's proposed reforms \(Pt II\): Privacy remedies](#)' *Privacy Laws & Business International Newsletter* 104, 10-12

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

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

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

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

Greenleaf, G (2009b) "Rudd Government abandons border security of privacy" *Australian Policy Online* 23 October 2009; [2009] ALRS 17

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

Greenleaf, G (2009d) 'Macao's EU-influenced Personal Data Protection Act' *Privacy Laws & Business International Newsletter*, 96, 21-22

Greenleaf, G (2008) 'Non-European states may join European privacy convention' *Privacy Laws & Business International Newsletter*, 94, 13-14

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

Greenleaf, G (2004) "Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners", http://papers.ssrn.com/sol3/papers.cfm?abstract_id=512782, accessed 2 September 2011

Greenleaf, G (2003) *Australia's APEC privacy initiative: the pros and cons of 'OECD Lite'*, *Privacy Law & Policy Reporter*, 10(10), 1–6; longer version available at <http://www2.austlii.edu.au/~graham/publications/2004/APEC_V8article.html>, accessed 2 September 2011

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*, 111, 7-8, July, 2011

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

- Hoofnagle, C (2010) 'Country Studies B.1 – United States of America' 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, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf, accessed 2 September 2011
- ICDPPC (2009) 31st International Conference of Data Protection and Privacy Commissioners 'Resolution on case reporting', adopted 5 November 2009, Madrid
- ICDPPC (2001) 23rd International Conference Of Data Protection Commissioners 'Accreditation Features Of Data Protection Authorities', adopted September 25, 2001, Paris
- Keane, J (2011) *The Life and Death of Democracy*, Pocket Books, 2011
- Korff, D and Brown, I (principal authors), and co-authors (including Greenleaf G) 'Final Report of the 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, http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, accessed 2 September 2011
- McLeish, R and Greenleaf, G (2008) 'Privacy in Hong Kong', Chapter in Rule and Greenleaf (2008)
- 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)
- Palazzi, P (2011) 'Data protection law in Latin America' (PPTs), presented at Privacy Laws & Business Annual Conference, Cambridge, July 2011
- Park, W (2008) 'South Korea' Chapter in Rule and Greenleaf (2008)
- Park, W and Greenleaf, G 'Korea reforms data protection Act' *Privacy Laws & Business International Report*, 109, 20
- Raab, C (2011) 'The meaning of "accountability" in the information privacy context' in Guagnin, D and others (Eds) *Managing Privacy Through Accountability*, Palgrave Macmillan, forthcoming 2011
- Rule, J and Greenleaf, G (Eds) *Global Privacy Protection: The First Generation*, Edward Elgar, Cheltenham, 2008
- Rule, J, Stearns, L, McAdam, D and Uglow, D (1981) *The Politics of Privacy: Planning for Personal Data Systems As Powerful Technologies*, Elsevier 1981
- Szekely, I 2008 'Hungary', Chapter in Rule J and Greenleaf G (2008)
- Waters, N (2008) 'The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection or a trojan horse for self-regulation?' [2008] UNSWLRS 59, <http://law.bepress.com/unswlrs/flrps08/art59/>, accessed 2 September 2011
- Waters, N (2011) 'The Asia Pacific Economic Cooperation (APEC) privacy framework - Implementation and enforcement: Moving forward or treading water' (PPTs), *Privacy Laws & Business Annual Conference*, St John's College, Cambridge, July 2011

ⁱ The assistance and contributions are acknowledged of Ian Brown, Lee Bygrave, Stewart Dresner, Marie Georges, Gus Hosein, Laura Linkomes, Jill Matthews, Charles Raab, Blair Stewart, and Nigel Waters. Responsibility for all errors and opinions remains with the author. This Chapter was completed while the author was the Inaugural CommonLII Fellow at the Institute of Advanced Legal Studies, University of London, July-August 2011, and was assisted by the opportunity to present some of its conclusions at the summer school of the Oxford Internet Institute in July 2011.

ⁱⁱ This part, and the table in the Appendix, is derived from my article ‘Global data privacy laws: Forty years of acceleration’ in (2011) 112 *Privacy Laws & Business International Report*, which contains more details explaining the table.