The Influence of European Data Privacy Standards outside Europe: Implications for Globalisation of Convention 108

Graham Greenleaf*
Abstract

Seventy-eight countries, from almost all regions of the world, have now enacted data privacy laws covering most of their private sectors. Enactment of laws outside Europe is accelerating. Before long, the majority of the world’s data privacy laws will be found outside Europe. This geo-political change has implications.

First, by examining the most important differences between the two European privacy standards (the EU Directive and the Council of Europe Convention 108) and the two non-European standards (the OECD Guidelines and APEC Framework), it is possible to identify what can reasonably be characterised as ‘European influences’ on data privacy laws outside Europe. Examination of the current 29 national data privacy laws outside Europe shows that the ‘European standards’ have had by far the greater influence outside Europe, and this is increasing.

Second, the Council of Europe data Protection Convention (Convention 108) and its Additional Protocol are examined from the perspective of the possibility and desirability of their becoming a global international agreement on data privacy. It is argued that there are potential considerable advantages to both non-European and European states if Convention 108 (plus the Additional Protocol) were to become a global privacy agreement through accession of non-European states. However, for such globalisation to occur, the Council of Europe will have to settle and publicise appropriate policies on accession that are appropriate, transparent, and do not reduce European data privacy standards.

Europe has no reason to retreat from its privacy standards developed over forty
years. The rest of the world is moving its way, and it should not compromise fundamental standards for the sake of compromise with powerful outliers, particularly the USA and China. Respect for their domestic prerogatives should not be confused with any need to reduce fundamental aspects of global data privacy standards.
The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales


Abstract: Seventy-eight countries, from almost all regions of the world, have now enacted data privacy laws covering most of their private sectors. Enactment of laws outside Europe is accelerating. Before long, the majority of the world’s data privacy laws will be found outside Europe. This geo-political change has implications.

First, by examining the most important differences between the two European privacy standards (the EU Directive and the Council of Europe Convention 108) and the two non-European standards (the OECD Guidelines and APEC Framework), it is possible to identify what can reasonably be characterised as ‘European influences’ on data privacy laws outside Europe. Examination of the current 29 national data privacy laws outside Europe shows that the ‘European standards’ have had by far the greater influence outside Europe, and this is increasing.

Second, the Council of Europe data Protection Convention (Convention 108) and its Additional Protocol are examined from the perspective of the possibility and desirability of their becoming a global international agreement on data privacy. It is argued that there are potential considerable advantages to both non-European and European states if Convention 108 (plus the Additional Protocol) were to become a global privacy agreement through accession of non-European states. However, for such globalisation to occur, the Council of Europe will have to settle and publicise appropriate policies on accession that are appropriate, transparent, and do not reduce European data privacy standards.

Europe has no reason to retreat from its privacy standards developed over forty years. The rest of the world is moving its way, and it should not compromise fundamental standards for the sake of compromise with powerful outliers, particularly the USA and China. Respect for their domestic prerogatives should not be confused with any need to reduce fundamental aspects of global data privacy standards.

* This paper was developed while the author was a Visiting Fellow at the AHRC-Script Centre, Faculty of Law, University of Edinburgh. An earlier version was presented to the International Data Protection Conference, Polish Data Protection Authority (GIODO), 21 September 2011, Warsaw. Parts of the paper are based on a chapter ‘Global data privacy in a networked world,’ to be published in the I Brown (Ed) Research Handbook on Governance of The Internet, Edward Elgar Publishing, Cheltenham, 2012 (in press). Very helpful comments were provided by (in alpha order) Inês Antas Barros, Colin Bennett, Lee Bygrave, Magda Cocco, Robert Gellman, Marie Georges, Chris Hoofnagle, Christopher Kuner, Pablo Palazzi, Jörg Polakiewicz, Charles Raab, Daniel Solove, Blair Stewart, and Nigel Waters, but responsibility for all content remains with the author. Assistance with the Table in this paper is acknowledged separately with the Table. Comments are welcome to <graham@austlii.edu.au>. A copy is at <http://www2.austlii.edu.au/~graham/>.
Greenleaf - The influence of European data privacy standards outside Europe

Contents

1 Introduction: Thinking globally ................................................................. 3
   International agreements, 'European' standards ...................................... 3
   The real world of data privacy laws: 78 countries and growing .......... 3
   Europe's data privacy laws will soon be outnumbered .......................... 4
   The outliers: The influence of the USA and China .............................. 4
   The USA's standards are fundamentally lower than Europe's ............ 5
   China's direction is unknown .......................................................... 7

2 The influence of 'European standards' ....................................................... 7
   The distinctiveness of the Directive ................................................... 7
   Influence of the 'European standards' in the 28 laws outside Europe ... 9
   The adequacy mechanism and 'border control' ................................. 12
   The strengthening Directive (and the Convention) ......................... 13

3 International agreements outside Europe ............................................. 14
   APEC's over-rated Framework and inchoate CBPR .......................... 14
   The ECOWAS data protection Act .................................................. 16
   Other regional agreements on data privacy ....................................... 16

4 CoE Convention 108 and Additional Protocol: A global agreement? .... 16
   Accession by non-CoE countries to Convention 108 ....................... 17
   The standards required by Convention 108, and 'modernisation' ......... 18
   'European standards' also requires accession to the Additional Protocol .. 19
   Problems with the procedures and standards for accession ............... 20
   The first example of non-European accession: Uruguay .................. 24
   Implications and advantages of accession for non-European states .... 25
   Advantages for European states in non-European accessions .......... 26

5 Conclusions ......................................................................................... 26
   Globalisation of Convention 108 is possible, but not inevitable .......... 26
   Europe should stick to its standards .............................................. 27

References ............................................................................................ 29
1 Introduction: Thinking globally

International agreements, ‘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 - the Convention for the protection of individuals with regard to automatic processing of personal data), both embodied privacy principles with many similarities but not identical substance, and expressed in somewhat different language.

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). The standards set by the Directive have become recognised as the strongest standard for data privacy in an international instrument. The Convention also now has an Additional Protocol (ETS No 181 – CoE, 2001) requiring data export limitations and supervisory authorities, so as to better align it with the Directive.

This paper considers the implications of these two key European privacy standards – Council of Europe Convention 108 (and its Additional Protocol) and the EU Directive – for countries outside Europe. But their implications for European countries are also changing.

The real world of data privacy laws: 78 countries and growing

In ‘Global data privacy laws: Forty years of acceleration’ (Greenleaf, 2011) the question ‘How many countries now have data protection laws?’ was answered with ‘76’, but the answer is now ‘78’ since Costa Rica adopted a data privacy law in September 2011, and Vietnam’s new consumer protection law (containing a privacy code) came into effect in July 2011. The unexpectedly high answer (the conventional answer was a somewhat vague ‘about sixty’ or perhaps ‘more than sixty’) has considerable implications for European privacy standards.

In the abovementioned analysis and its accompanying Table, a country is only considered to have a ‘data privacy law’ if it has a national law which provides, in relation to most aspects of the operation of the private sector, a set of basic data privacy principles, to a standard at least approximating the OECD Guidelines, plus some methods of statutorily-mandated enforcement (ie not only self-regulation). Countries that have national public sector laws but no comprehensive private sector laws (only the USA and Thailand are known) are therefore excluded. Almost all the 78 jurisdictions have laws which also cover their national public sectors (the only exceptions being Malaysia, Vietnam and India), possibly by different legislation to that covering the private sector. Therefore, there are 75 countries providing comprehensive coverage of both their private and public sectors. Almost all of these jurisdictions provide in their legislation for a Data Protection Authority (DPA), a separate institution with responsibility for the data privacy legislation, although these vary greatly in name, functions and degree of independence from other government authorities. Chile, the Kyrgyz Republic, India, Japan, Vietnam and Taiwan are the few remaining exceptions with no DPA.
The total number of new data privacy laws globally, viewed by decade of enactment, shows that their growth is accelerating, not merely expanding linearly: 7 (1970s), 10 (1980s), 19 (1990s), 32 (2000s) and 10 (1.75 years of 2010s), giving the total of 78. In the first 21 months of this decade 10 new laws have been enacted (Faroe Islands, Malaysia, Mexico, India, Peru, Russia - more accurately, brought into force – Ukraine, Angola, Vietnam and Costa Rica), making this the most intensive period of data protection developments in the last 40 years. By region, the distribution of laws is in order: European Union (27); other European Countries (22); non-European countries (28) (Asia (8); Latin America (7); Sub-Saharan Africa (6); North Africa and Middle East (3); Australasia (2); North America (1); Caribbean (1); Central Asia (1); and Pacific Islands (0)). There are Bills or proposed Bills for new data privacy laws in many countries, including Brazil, Ghana, South Africa, Thailand, the Philippines and Singapore. At the current rate of growth, there may be more than 80 data privacy laws by early 2012.

Europe’s data privacy laws will soon be outnumbered

The 22 European separate jurisdictions which are not EU member states but do have data privacy laws are: Albania; Andorra; Azerbajain; Bosnia & Herzegovina; Croatia; Faroe Islands; FYROM (Macedonia); Gibraltar; Guernsey; Iceland; Isle of Man; Jersey; Liechtenstein; Montenegro; Moldova; Monaco; Norway; Russia; San Marino; Serbia; Switzerland; and Ukraine. So there are a total of 50 European data privacy laws. There is little room for expansion within Europe: Armenia, Georgia, Turkey and Belarus are the only remaining European states without data privacy laws.

Most expansion of data privacy laws is now occurring outside Europe. There are now 29 data privacy laws outside Europe (see the Table following), more than the number of countries in the EU. In a few years, when the total of countries with data protection laws is likely to pass 100 (assuming the current rate of 5 or 6 new laws per annum, almost all from outside Europe), Europe as a whole will be in the minority of countries with data privacy laws. This geopolitical fact has considerable implications for both the Directive and Convention 108.

The outliers: The influence of the USA and China

The two major exceptions to the development of comprehensive data privacy laws, in terms of global political and economic influence, are the USA and China. The economic and political power of both counties requires special consideration in any assessment of global data privacy developments. However, the increasing isolation of their positions must also be recognised. Most other countries that do not have (or clearly plan to have) data privacy laws have relatively limited global influence although some (eg Indonesia and Nigeria) have substantial populations. In Latin America, Africa, and Asia, a steady expansion in the number of countries adopting data privacy laws seems likely. In the Middle East and Central Asia, such laws are starting to emerge. Most of the rest of the world is increasingly adopting a generally consistent set of principles and establishing a DPA as part of the enforcement mechanism, as is demonstrated in the next part of this paper. 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-sponsored APEC-supported alternatives which might have impeded the spread of strong data privacy laws in Asia and Latin America largely appear to have failed. There is nothing occurring in the rest of the world which represents a coherent alternative to the spread of European-influenced data privacy standards, or even coherent resistance (except in the USA) to the adoption of such standards.
The USA’s standards are fundamentally lower than Europe’s

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 major companies and Bills introduced into Congress. It is not the case that the USA does not have any standards for private sector data privacy, but they must be inferred from many scattered pieces of sectoral legislation, the absence of any significant legislation in many sectors (just as important), some State constitutional protections, and the common law. Concerning the last of these, the USA’s privacy torts, despite their fame, are only capable of sporadic contributions to data privacy (Solove, 2004: 57-62). 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. The Federal Trade Commission (FTC) has gradually adopted the broadest role (though still in relation to only the parts of the private sector where it has jurisdiction, under its authority to counter ‘unfair trade practices’, particularly online misrepresentation concerning the purpose of collection of personal information and assurances of data security. But its reach is limited to ensuring that companies keep the promises they make in their privacy policies or otherwise (Solove, 2004: 73) and (though rarely used) unfairness cases. However, as Hoofnagle says, even within its limited ambit, '[i]t 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'. Hoofnagle 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’. The protection of privacy-affecting marketing as ‘free speech’ goes beyond what is accepted in many other countries. Although the Federal Privacy Act (1974) applied most of the pioneering HEW principles of 1973 to the federal public sector, including the ‘purpose limitation’ principle that information collected for one purpose should not be used or made available for other purposes without consent (Regan, 2008: 56), little of the main subsequent legislation applying to the private sector has applied this principle (Regan, 2008: 57-60; Solove, 2004: 67-72). The result is a patchwork of inadequate laws that, in any event, ‘only cover a small geography of the database problem’ (Solve, 2004: 71).

There is therefore an arguable case that, even if all of the USA’s existing sectoral laws (including FTC protections and privacy torts) were consolidated into one Act, and even if that Act was extended to the whole of the private sector, the standards it would embody would fall short of European standards in fundamental respects. The lack of general application of purpose limitation principles makes it questionable whether the USA has even complied with the OECD guidelines in relation to its private sector. The lack of laws limiting collection to the minimum data required for a legitimate purpose is a further difference from fundamental European standards (at least on paper: criticism of weak enforcement is justified). US data privacy laws enacted in the USA may be weaker on these points than European laws not only as a matter of fact, but also as a matter of constitutional necessity. This is because the First Amendment to the US Constitution is likely to make it unconstitutional for the federal
government to impose some restrictions on disclosure, use and collection of personal information by the private sector (and perhaps by the States). Regan argues that any US privacy legislation is likely to be challenged in the courts, including ‘on the basis of First Amendment grounds that any information, including that about individuals, should flow freely and without government restriction’ (Regan, 2008: 51). Hoofnagle, however, considered that since US West v FCC (1999) held that opt-in consent restrictions on secondary use of telephone records violated commercial free speech rights (with which another circuit court has disagreed), subsequent court decisions ‘have consistently upheld data-protection-style privacy laws against First Amendment challenges’ (Hoofnagle, 2010: 7).

Other scholars had taken a more negative position that the First Amendment protects a right to gather information (Froomkin, 2000: 1508), questioning the correctness of the Supreme Court’s decision in *Reno v Condon* which upheld a federal law limiting access to personal information in the drivers’ licence databases maintained by the fifty states. Hoofnagle’s more positive assessment has now been made very doubtful by the U.S. Supreme Court’s recent decision in *Sorrell v. IMS Health Inc.*, 131 S.Ct. 2653, 2672 (2011), which found that a state law that prohibited the sale of information on doctors’ prescribing habits to marketers for drug companies violated the First Amendment (Julin, 2011). In relation to the Do-Not-Track bills currently before Congress, it has been argued that the principles of this case ‘strongly suggest that any such legislation would run afool of the First Amendment’ (Julin, 2011), but other more narrow readings of the decision are also possible. The full scope of constitutional limitations on the possibility of data privacy laws in the USA is clearly not yet settled, but it seems that they are a significant if uncertain limitation (perhaps an example of a ‘known unknown’). It is beyond the scope of this paper to demonstrate the scope of either the actual or potential limits on US data privacy laws, but it is important to state that there is a arguable case that US privacy standards have both actual and inherent limitations which place them at odds with fundamental aspects of European privacy standards.

These limitations do not mean that the USA lacks privacy standards or privacy innovations. In recent years there has been a profusion of innovative state laws in areas such as data breach notification and laws to limit effects of identity theft. Nor does it lack examples of effective enforcement. The high financial settlements often imposed by the Federal Trade Commission (FTC) on the basis of sectoral laws on deceptive practices amount to around US$40 million in fines (Hoofnagle’s estimate), which is still not a substantial amount given the revenues of the companies concerned, but the concomitant damage to reputation may be far more substantial. R E Smith (2011) gives a succinct but lengthy catalog of where US laws have pioneered particular privacy protections, often with laws that are stronger than elsewhere. These laws are significant, but don’t add up to anything like a comprehensive data privacy law, or a coherent alternative set of policies to protect data privacy.

The main point being made here is that the USA’s exceptional position 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 arising from circumstances which may be unique to the USA) and no national DPA as a key means of enforcement. The USA is best seen as a country with a unique, largely isolated and sometimes inconsistent approach to data privacy, with some key standards weaker than is common in the rest of the world (particularly limits on collection, secondary use, disclosure and data exports). But it also often provides international innovation 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. However, the USA does not provide an alternative paradigm for data privacy that deserves an undue amount of respect simply because of its economic and political power.
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 may now be on the wrong side of history.

The rest of the world has to accept that there are some aspects of US domestic law on data privacy which are unlikely to change, but that does not constitute a reason for reducing international privacy standards in fundamental ways in order to accommodate or compromise with the inherent or deliberate weaknesses of American privacy protection. That would merely be capitulation.

**China’s direction is unknown**

China is the other major power where there is little sign of a national data privacy law covering the private sector (Greenleaf, 2011a). In 2006-7, an EU-style draft Personal Information Protection Act was under consideration, covering both the private and public sectors, but this no longer seems to be favoured, and the Informatics Committee of the State Council considering it has been abolished. Instead, in recent years a profusion of different types of laws have been enacted. These give only partial coverage: the Seventh Amendment to the Criminal Law (2009) criminalised a wide range of disclosures of personal information and the obtaining of same; the PRC Tort Liability Law (in force 2010) includes a right to privacy (隐私权) in its list of protected ‘civil rights and interests’, but without defining further what is meant; data privacy provisions have been included in sectoral laws and guidelines in 2009/10 the fields of money laundering, medical records, insurance, consumer protection and credit reporting; various Provinces have also enacted local data privacy codes, particularly in consumer law; and the Ministry of Industry and Information Technology (MIIT) Standardization Administration of China (SAC) has issued draft non-enforceable ‘Guidelines for Personal Information Protection’ (2011). These initiatives are piecemeal and incoherent. If they are eventually replaced or supplemented by a national data privacy law, China may well influence developing countries and China’s trading partners. But no-one knows the direction China will take.

2 **The influence of ‘European standards’**

What does it mean to say that ‘European standards’ for data privacy have been influential? How can we measure that? Can we identify the causes of influence, or only the effects?

**The distinctiveness of the Directive**

With a very small number of exceptions (Israel, public sector laws in some OECD countries, New Zealand) data protection laws outside Europe post-date the 1995 Directive (or at least post-date its draft form in the early 90s) and were therefore open to its influence at their inception. In some cases revised laws (eg Taiwan, South Korea, New Zealand) have added new elements influenced by the Directive.

To argue that a law outside Europe is influenced by the EU Directive of 1995, rather than by the preceding developments of the OECD Guidelines or the subsequent development of the APEC Privacy Framework, it is first necessary to identify those elements which are found in the Directive (and in some cases also in Convention 108) but are not required by the OECD Guidelines or the subsequent APEC Framework (in general, a weaker version of the OECD Guidelines: Greenleaf, 2003, 2009c). The following list of the ten most significant differences...
between the European instruments and the OECD/APEC instruments is not comprehensive but is indicative of the higher standards that one or both embody (informed in part by Bygrave, 2008, 19-38):

1. Requirement of an independent Data Protection Authority as the key element of an enforcement regime (EU Directive, and Additional Protocol to Convention 108);

2. Requirement of recourse to the courts to enforce data privacy rights (EU Directive, Convention 108 and more explicitly the Additional Protocol to Convention 108);

3. Requirement of restrictions on personal data exports to countries which did not have a sufficient standard of privacy protection (defined as ‘adequate’) (EU Directive, and Additional Protocol to Convention 108);

4. Collection must be the minimum necessary for the purpose of collection, not simply ‘limited’ (both EU Directive and Convention 108);

5. A general requirement of ‘fair and lawful processing’ (not just collection) (both EU Directive and Convention 108); where a law outside Europe adopts the terminology of ‘fair processing’ and a structure based on other obligations being instances of fair processing, this is both indicative of influence by the Directive, and makes it easier for the law to be interpreted in a way which is consistent with the Directive;

6. Requirements to notify, and sometimes provide ‘prior checking’, of particular types of processing systems (EU Directive);

7. Destruction or anonymisation of personal data after a period (both EU Directive and Convention 108);

8. Additional protections for particular categories of sensitive data (both EU Directive and Convention 108);

9. Limits on automated decision-making, and a right to know the logic of automated data processing (EU Directive);


Other ‘European’ elements could be added to this list, for example the right to prevent further processing, but the above choice has been made on the basis that these are the ten most important distinguishing elements. None of these ten elements is required, or even recommended, by the OECD Guidelines or APEC Framework. The as-yet incomplete APEC CBPR initiative may include some of these elements, but is irrelevant as influences are not retrospective. It is plausible to argue that non-European laws including a significant number of these ten elements are ‘primarily influenced by the EU Directive’.

In order to be comprehensive, the same analysis would need to be made for the influences of each of the following (i) the elements that are distinctive to the APEC privacy framework (discussed later); (ii) the elements shared by the OECD Guidelines and the Council of Europe Convention 108 (which account for much of the similarities of all data privacy laws, but are not analysed in this article); and (iv) the elements in national privacy laws which are not found in any of these international agreements.
**Influence of the ‘European standards’ in the 28 laws outside Europe**

A systematic analysis of the effect of European privacy standards outside Europe requires the analysis of the (currently) 28 privacy laws outside Europe to determine the extent to which the ten factors above are found in those laws, and this is attempted in the following Table.

This Table only indicates correlations between the contents of a national law and the suggested ‘European’ elements. The question of causation, whether the provisions found in the Directive or Convention 108 either directly or indirectly caused (or more accurately, influenced) the adoption of a similar provision in a non-European law, can only be answered by detailed national studies (in the domains of legal history, politics or sociology) of the influences brought to bear in the enactment of particular legislation. An a-historical analysis such as is provided by this Table can only give rise to plausible hypotheses which invite further investigation and evidence. At best, we could argue that if the correlations are strong enough, they might give rise to a presumption that European influence is involved, rebuttable by further investigation.

In some cases, national laws are more strict than the European requirements, and this is still counted as providing the European element by going beyond it. For example, South Korea requires consent for all data exports, with no automatic right to export data to ‘adequate’ jurisdictions. Korea also requires consent (ie ‘opt in’) for any direct marketing uses of personal data. On the other hand, just because the right words are used does not mean a provision is present: the Indian Rules refer to ‘sensitive’ information, but do not in fact prescribe a class of information to be given more extensive protection, so this does not count.

In some cases, provisions in laws have not yet been brought into force, but these have still been counted in this analysis. For example, Hong Kong has a data export provision not yet in force. Malaysia has not yet appointed a Privacy Commissioner under its legislation. Some assessment for the Table are matters of interpretation and opinion: for example, whether New Zealand law has the requisite type of data export provisions, or the requisite limits on automated decision-making, are matters of interpretation, but I have followed the approach taken by the Expert Report on New Zealand accepted by the Article 29 Committee.

The more correlations there are between a law and the European elements, indicated by the number (0-10) in the final column, the more it is suggestive of a conscious influence of the Directive in a particular country. For example, the score of 9 for Macau is no surprise, given that it is known to be based on the Portuguese law. The score of 9 for South Korea is perhaps more surprising, given that its law is not known to be based closely on that of any particular European country, although German law has had some influence.

The Table, and the total scores for a country, do not say anything much about whether a country's law is likely to be regarded as ‘adequate’ by the European Union. Adequacy assessments take into account different factors, and do not only consider the formal law, but also its implementation in practice. The question of whether a country's law makes it appropriate for that country to accede to Convention 108 is also a quite different question to which different standards apply (see discussion later). It seems to be common sense that it would be more profitable to investigate (from the perspectives of potential adequacy or potential accession) a country whose law shares nine of these European elements, rather than one whose law only shares a couple of them. However, it is quite possible that a law with a high number of ‘European’ elements might also have broad exemptions to its principles, and major deficiencies in its enforcement procedures, so the Table and its numerical summary also cannot be simply equated with the ‘strength’ of a data privacy law.
**Table: Indicators of European influences on non-European data privacy laws**

This table lists the 29 known data privacy laws outside Europe as at October 2011.

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Key Act</th>
<th>Latest</th>
<th>Region</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>Ttl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peru</td>
<td>Law on Protection of Personal Data</td>
<td>2011</td>
<td>Latin Am</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Uruguay</td>
<td>Law on the Protection of Personal Data</td>
<td>2008</td>
<td>Latin Am</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Burkina Faso</td>
<td>Law on Protection of Personal Information</td>
<td>2004</td>
<td>Africa</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Senegal</td>
<td>Act on the Protection of Personal Data</td>
<td>2007</td>
<td>Africa</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Morocco</td>
<td>Data Protection Act</td>
<td>2009</td>
<td>M.East/N.Af</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Angola</td>
<td>Lei da Protecção de Dados Pessoais</td>
<td>2011</td>
<td>Africa</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Argentina</td>
<td>Personal Data Protection Act</td>
<td>2000</td>
<td>Latin Am</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Macau SAR</td>
<td>Personal Data Protection Act</td>
<td>2007</td>
<td>Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>South Korea</td>
<td>Data Protection Act</td>
<td>2011</td>
<td>Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>9</td>
</tr>
<tr>
<td>Mauritius</td>
<td>Data Protection Act</td>
<td>2004</td>
<td>Africa</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>Protección de la Persona frente al tratamiento de sus datos personales</td>
<td>2011</td>
<td>Latin Am</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Benin</td>
<td>Loi sur la Protection des données personnelles</td>
<td>2009</td>
<td>Africa</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Cape Verde</td>
<td>Loi N° 133/V/2201 du 22 janvier 2001</td>
<td>2001</td>
<td>Africa</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>Colombia</td>
<td>Data Protection Law</td>
<td>2008</td>
<td>Latin Am</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Tunisia</td>
<td>Law on the protection of personal data</td>
<td>2004</td>
<td>M.East/N.Af</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Personal Data Protection Act</td>
<td>2010</td>
<td>Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Personal Data Protection Act</td>
<td>2010</td>
<td>Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>Canada</td>
<td>Personal Information Protection and</td>
<td>2002</td>
<td>North Am</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>7</td>
</tr>
</tbody>
</table>

---

1 The completion of the Table is based on advice received in relation to Latin American countries from Pablo Palazzi (Allende & Brea, Argentina); in relation to francophone countries, from Marie Georges (Planete Informatique et Liberties, Paris); in relation to lusaphone (Portuguese-speaking) countries, from Magda Cocco and Inês Antas Barros (Vieira de Almeida & Associados, Lisbon); and in relation to Canada, from Colin Bennett (Victoria University, BC); overall responsibility remains with the author. Articles supporting many of these assessments are in the bibliography.

http://law.bepress.com/unswwps-flrps11/art42
Greenleaf - The influence of European data privacy standards outside Europe

<table>
<thead>
<tr>
<th>Country</th>
<th>Act/Ordinance</th>
<th>Year</th>
<th>Region</th>
<th>EU1</th>
<th>EU2</th>
<th>EU3</th>
<th>EU4</th>
<th>EU5</th>
<th>EU6</th>
<th>EU7</th>
<th>EU8</th>
<th>EU9</th>
<th>EU10</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hong Kong SAR</td>
<td>Personal Data (Privacy) Ordinance</td>
<td>1995</td>
<td>Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>7</td>
</tr>
<tr>
<td>Australia</td>
<td>Privacy Act 1988</td>
<td>2001</td>
<td>Australasia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Privacy Act 1993</td>
<td>2010</td>
<td>Australasia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
</tr>
<tr>
<td>Kyrgyz Rep.</td>
<td>Law on Personal Data</td>
<td>2008</td>
<td>Central Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
</tr>
<tr>
<td>Mexico</td>
<td>Federal Law on the Protection of Personal Data Held by Private Parties</td>
<td>2010</td>
<td>Latin Am</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>5</td>
</tr>
<tr>
<td>India</td>
<td>s43A Rules, Information Technology Act 2000</td>
<td>2011</td>
<td>Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>4</td>
</tr>
<tr>
<td>Israel</td>
<td>Privacy Protection Act 1981</td>
<td>1981</td>
<td>M.East/N.Af</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>4</td>
</tr>
<tr>
<td>Bahamas</td>
<td>Data Protection Act</td>
<td>2003</td>
<td>Caribbean</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>3</td>
</tr>
<tr>
<td>Japan</td>
<td>Act on the Protection of Personal Information</td>
<td>2003</td>
<td>Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>1</td>
</tr>
<tr>
<td>Chile</td>
<td>Privacy Law</td>
<td>1999</td>
<td>Latin Am</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>1</td>
</tr>
<tr>
<td>Vietnam</td>
<td>Law on Protection of Consumers' Rights</td>
<td>2011</td>
<td>Asia</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>1</td>
</tr>
</tbody>
</table>

**Totals** | 22 | 23 | 25 | 21 | 20 | 16 | 24 | 25 | 13 | 20

**Key to numbered columns of ‘European’ elements:**
1. Has an independent Data Protection Authority (DPA);
2. Allows recourse to the courts to enforce data privacy rights;
3. ‘Border control’ restrictions on personal data exports to overseas countries;
4. Collection must be the minimum necessary for declared purposes;
5. General requirement of ‘fair and lawful processing’;
6. Requirements to notify DPA, and provide ‘prior checking’ of some processing systems;
7. ‘Deletion’: Destruction or anonymisation of personal data after a period;
8. Additional protections for particular categories of sensitive data;
9. Limits on automated decision-making (incl. right to know logic of automated processing);
10. Requirement to provide ‘opt-out’ of direct marketing uses of personal data.

What we can see from the Table is that of the 29 African, Latin American, Asian, Australasian, and other jurisdictions with data privacy laws, all jurisdictions except four (Japan, Bahamas, Vietnam and Chile) have at least four of the ten ‘European’ elements. Nineteen of the 29 have 7 or more elements, and 13 of the 29 have at least nine of the ten elements. This last group is geographically diverse, including Peru, Burkina Faso, Argentina, Macau, Morocco, Angola, South Korea and Mauritius. I suggest this leads to quite a strong inference that European privacy standards have been, either directly or indirectly, influential in all of these Latin American, Asian, African and Australasian countries except the four with 3 or fewer where the influences are minor. The influences are modest (a score of 4) in Israel (a 1981 law that pre-dates the Directive and is a contemporary of the Convention) and India (a set of rules inserted into another Act).
All the ten ‘European’ elements of data privacy laws identified above are found in at least 13 data privacy laws outside Europe: the least common features are limits on automated decision-making (13/29) and requirements for prior checking of some systems (16/29). Some are commonplace, for example specialist data protection agencies (22/29); ‘border-control’ data export restrictions (25/29); additional protection for sensitive data (25/29); deletion requirements (24/29). Some elements also appear in unexpected places (eg ‘fair and lawful processing’ in Malaysia). The average number of times each feature appears is 20.9/29 instances, so on average each ‘European’ feature is present in over two thirds (almost three-quarters) of all non-European data privacy laws.

Of course, it is logically possible (although quite implausible) that these ‘European’ elements have been independently invented, time and again, in non-European states. More realistically, Raab (2010) explains some of the likely patterns of influence in his study of the complex interactions between European data protection authorities and policy-makers in non-European countries with similar linguistic backgrounds, such as the Ibero-American Data Protection Network (RedIPD) and the Association of Francophone Data Protection Authorities (AFAPDP). There is also a lusophone network. Only fully detailed studies of the history of data privacy laws in particular countries, such as the country studies in Rule and Greenleaf (2008) can properly answer questions about influences. In three countries examined there, outside the networks considered by Raab, Australian and Hong Kong laws showed evidence of influence by the EU Directive. The study of the then Korean law did not (though factors such as data export restrictions were present), but the 2011 revised Korean law shows stronger EU influence (Greenleaf, 2011a). Bennett and Raab’s analysis of the emergence of data privacy laws up to 2005 (2006, Ch 5) also sees significant influence of the Directive both in Europe outside the EU and in non-European laws, but not to the extent identified here.

On the basis of what is shown in this Table, which is consistent with expert but impressionistic knowledge of the contents of these laws, we can say that outside Europe, something reasonably described as ‘European standard’ data privacy laws are becoming the norm in most parts of the world with data privacy laws. This trend is most noticeable in Latin America, with Costa Rica recently joining Argentina, Colombia and Uruguay with EU-style laws, and Mexico with a law with both EU and OECD influences. 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). Macau’s law is derived directly from the Portuguese law. Japan, Hong Kong, New Zealand (likely to soon be the second Asia-Pacific country after Canada found to be ‘adequate’) and Australia (where protracted law reform processes 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, even Vietnam where the influence is more clearly from the OECD than from APEC (see later, and generally Greenleaf, 2011a and articles cited therein for evidence for specific countries).

Although more evidence of causation is desirable, it is an entirely plausible (and in my view, correct) hypothesis that the EU Directive is the most significant overall influence on the content of data privacy laws outside Europe, and that its influence is gradually strengthening, partly because of the desired of non-EU countries to have their laws recognised as ‘adequate’, but also because of the their aspiration that their laws should be recognised as providing the highest international standard of privacy protection.

The adequacy mechanism and ‘border control’
The ‘adequacy’ mechanism in the Directive, and perceptions of it outside Europe, have been one (but only one) of the means by which the influence of European standards has been felt.
Greenleaf - The influence of European data privacy standards outside Europe  

The EU’s ‘border control’ approach is to require member states 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' (EU Commission, 2010, 2.4.1). There is a further problem that different EU Member States make different judgments on adequacy.

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), some of which are of little economic or political significance. Uruguay and New Zealand will soon be added to this list, following positive findings by the increasingly pragmatic Article 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.

There could be significantly more adequacy findings outside Europe if the EU was more pro-active and more transparent about its processes. Where the EU has made positive adequacy decisions it has publicised the reasons, but where it has considered ‘applications’ from other countries but concluded that their protections were not yet adequate, it has not generally publicised the reasons for these negative conclusions. There has therefore been much less information available about what does and does not constitute ‘adequacy’ than is desirable. Individual European countries do not seem to have blocked particular data exports very frequently since the Directive has been in force, thus reducing the impact of the adequacy requirement. However, whether these has been less blocking of data exports than occurred during the 1980s and early 1990s (when there seemed to be quite a lot) needs empirical verification. There has also been considerable criticism of whether EU countries live up to their own standards, including assertions of considerable inconsistency and non-enforcement by EU members in relation to the data export provisions (Bygrave 2010, p 197).

Despite the slow pace of the EU in making and publicising 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).

Outside Europe, 'border control' data export limitations are found almost all (25/29) data privacy laws in all regions, though their strength varies a great deal, and they are not yet in force in the laws of Malaysia and Hong Kong. So anyone who wishes to criticise the EU for wanting to 'impose its standards on the rest of the world' had better level the same accusation at the rest of the world.

**The strengthening Directive (and the Convention)**

Fifteen years after 1995, 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 in Greenleaf (2011). 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, some of the emergent international data privacy norms that the Commission is considering (such as data breach notification, the ‘right to be forgotten’ and ‘data portability’), and other innovations, 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 protected in India’s new law. These examples are only from the Asia-Pacific, but similar ones may well be found in Latin America and Africa. 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.

3 International agreements outside Europe

Some international data privacy agreements outside Europe will be significant, but probably not the one that usually comes to mind.

APEC’s over-rated Framework and inchoate CBPR

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, and overlapping the Council of Europe by inclusion of Russia), 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, the APEC processes have 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 Privacy Principles (Part III of the Framework) contain three Principles which it can be argued are not explicitly found in the two European instruments: ‘Preventing Harm’ (Principle I); ‘Choice’ (Principle V); and ‘Accountability’ concerning data exports (Principle IX). While it can be argued that these are not valuable additions to sets of privacy principles (Greenleaf, 2008), the separate question relevant to this paper (and as asked above about the ‘European’ principles) is whether these three ‘APEC Principles’ have had any influence on the development of national privacy laws, particularly those outside Europe. The short answer is that their influence appears to be minimal. New Zealand had a provision (not a Principle) which could be recognised as ‘preventing harm’ before the APEC Framework existed, and Canada had an ‘accountability’ principle relevant to data exports. Vietnam has none of the ‘APEC trio’, although otherwise it joins Japan as the least ‘European’ of Asian laws. There are possible future influences coming from law reform reports and Bills (‘accountability’ in Australia or New Zealand) but these might not become legislation. The Mexican law does include a version of the APEC ‘accountability’ principle. The ‘choice’ principle is not explicitly included in any national data protection principles, and it is difficult to assess whether it is impliedly and diffusely implemented anywhere. Perhaps other examples can be found, but it seems clear that, compared with the widespread influence of the distinctive aspects of the ‘European’ principles, the distinctive APEC principles have gained little traction.

The APEC approach was initially enthusiastically supported by at least the USA, Australia, Canada and Mexico, and acquiesced in by other countries. However it has failed to establish an alternative paradigm for data protection: almost no evidence of adoption of its principles in legislation in the region; little increase in self-regulatory initiatives (there are privacy seals in Mexico, Vietnam and Japan, but they are of questionable value); and a faltering CBPR initiative (Greenleaf, 2008; Waters, 2008, 2011, 2011a). New laws in the region are influenced more by the EU Directive than by the APEC Framework, as discussed previously.

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. However, it is necessary to distinguish the APEC CBPR initiative for a number of reasons: (i) it does include elements not found in the APEC Framework (eg a requirement that CBPR be underpinned by local legislation); and (ii) it is possible that it could have some future effectiveness. However, those factors are not directly relevant to the argument in this paper, which is primarily about what has influenced non-European laws up until now: influences cannot be retrospective.

Even the best global analyses of data privacy developments still tend to accord too much significance to the APEC Framework as a brake on European influence (eg Bennett & Raab, 2006; Bygrave, 2008, 2010). It is more likely that APEC will be seen as a dead-end: why pay
attention to non-binding guidelines that no-one follows and (probably) CBPR rules that have almost no implementation?

While this paper emphasises the points of difference or distinction between the ‘European’ and ‘non-European’ (OECD and APEC) international agreements, and takes the view that those differences are very significant in substance (Greenleaf 2008) and that Europe should not ‘trade down’ in order to achieve some global consensus, other commentators argue that the differences are much less significant in substance (Waters, 2008) and therefore tend to be more optimistic about a possible global consensus. It is beyond the scope of this paper to reconsider all of those arguments. However, what is unarguable is that there is a great deal of common ground between the European and non-European principles, and this commonality helps to explain the remarkable overall consistency of the world’s 76 national data privacy laws (and many sub-national laws as well).

The ECOWAS data protection Act
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 specifies the required content of such data privacy laws, influenced very strongly by the EU Directive, and that each state must establish a data protection authority. As noted earlier, four ECOWAS states have enacted such laws (Benin, Burkina Faso, Cape Verde, and Senegal), and a Bill is before Parliament in Ghana.

Other regional agreements on data privacy
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.

4 CoE Convention 108 and Additional Protocol: A global agreement?
Council of Europe (CoE) Convention108 (the Convention for the protection of individuals with regard to automatic processing of personal data) Articles 5-8 are a set of data privacy principles that, while stated briefly, do contain versions of most of the elements we now recognise as core data privacy principles. Many of the principles are similar to those found in the OECD Guidelines due to cross-influences between the drafters of the two instruments. However, the Convention contains few of the enforcement mechanisms now regarded as essential.

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 therefore 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).

Forty-three CoE member States have ratified the Convention, and have data privacy laws (see the Table in Greenleaf, 2011 or the CoE accessions page). Armenia, Turkey and the Russian
Federation have signed but not ratified the Convention. San Marino has done neither. However, Russia does now have a data privacy law (in force 2011). Armenia, Georgia and Turkey are the only Council of Europe Member State not to have enacted a data privacy law. Belarus is not a Council of Europe member because of human rights concerns, and the Vatican (Holy See) is not a member because it is not a democracy. The UK and other countries have acceded to the Convention on behalf of their self-governing territories.

Thirty-one European countries have also ratified the Additional Protocol (see the Table in Greenleaf, 2011 or the CoE accessions page). 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.

**Accession by non-CoE countries to Convention 108**

Article 23(1) has provided for accession by non-member States since 1981: ‘... the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee’. However, the Committee of Ministers had not invited a State to accede for the first quarter-century of the Convention’s life.

The world’s privacy and data protection Commissioners at their 27th International Conference in Montreux, Switzerland (2005) gave this aspect of Convention 108 a wake-up call when they agreed on a concluding ‘Montreux Declaration’ which issued a number of challenges to global organizations and national governments. One was their appeal ‘to the Council of Europe to invite, in accordance with article 23 [of Convention 108 on data protection] ... non-member-states of the Council of Europe which already have a [sic] data protection legislation to accede to this Convention and its additional Protocol.’ Article 23 had lain dormant while the CoE concentrated on obtaining accessions to Convention 108 from all of the European members of the CoE. The Secretary General took note of the Declaration and expressed his willingness to promote the Convention internationally.

In March 2008 the Consultative Committee of the Convention (T-PD) at its 24th annual meeting, considered accession of non-Member States under Article 23. According to its minutes (CoE 2008):

53. Lastly, the representative of Switzerland recalled the final declaration of the Montreux Conference of Privacy Commissioners in 2005, which had called the Council of Europe to “invite, in accordance with article 23 of the Convention for the protection of individuals with regard to automatic processing of personal data, non-member states of the Council of Europe which already have data protection legislation to accede to this Convention and its additional Protocol”. He considered that now would be a good time for the Council of Europe to issue such an invitation, as these accessions could be a step towards a much called-for universal right to data protection which is becoming all the more important in today’s world of borderless telecommunication networks. They would also contribute to reinforce the Council of Europe’s visibility in this area.

54. The T-PD agreed and therefore recommended that non-member states, with data protection legislation in accordance with Convention 108, should be allowed to accede to the Convention. It invited the Committee of Ministers to take note of this recommendation and to consider any subsequent accession request accordingly.
The Committee of Ministers at its 1031st meeting on 2 July 2008 (CoE 2008a), meeting at Deputy level, made the following Decisions:

1. took note of the T-PD’s recommendation that non-member states with data protection legislation in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) should be allowed to accede to this convention;
2. agreed to examine any accession request in the light of this recommendation;
3. instructed the Secretariat to disseminate information about the convention;
4. took note of the abridged report of the 24th plenary meeting of the T-PD as a whole, as it appears in document CM(2008)81.

From mid-2008, non-European accession to the Convention therefore became possible as a matter of practicality. However, ‘[t]he Council of Europe never really promoted the Convention outside Europe. It was only in December 2009 that the EU's Stockholm Programme explicitly called for the promotion of Convention 108 worldwide’ (Polakiewicz 2011). This promotion is now underway. Uruguay ‘may become a party later this year’ (Polakiewicz 2011). The CoE is actively involved in discussions with other states, some of which have indicated informally their interest in acceding. But whether the CoE is likely to succeed in turning Convention 108 into a global convention is still an open question, on which this article is intended to shed some light.

Global conventions originating from Europe are not unprecedented, and some other Council of Europe Conventions are open to ratification by non-Member State. For example, the Cybercrime Convention has been ratified by the USA, and signed by three other non-European states (South Africa, Japan and Canada). Accession is now being promoted vigorously by the CoE and other parties, and countries like Australia have passed legislation to enable accession.

**The standards required by Convention 108, and ‘modernisation’**

How high is the standard of data privacy that non-European states must meet in order to accede to the Convention and the Additional Protocol (both are required, as discussed below). It is necessary to consider both data protection principles and how they are enforced. The Convention applies to automated processing of personal data, but parties may extend its application to other categories of data. The Convention was amended in 1999 (Council of Europe, 1999) to allow the European Communities to accede.

First, concerning principles, Articles 5-8 of Chapter II set out Convention 108’s data protection principles in what Bygrave (2008) rightly describes as ‘broad brush fashion’. Most of the work is done by Article 5 (Quality of data) which requires that:

- Personal data undergoing automatic processing shall be: 1. obtained and processed fairly and lawfully; 2. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; 3. adequate, relevant and not excessive in relation to the purposes for which they are stored; 4. accurate and, where necessary, kept up to date; 5. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Other than that, all that Chapter II includes are familiar principles requiring ‘appropriate’ data security (Article 7), and rights to ascertain the existence of personal files, to access them, and to correct them (Article 8). There is also a provision for ‘sensitive’ data in Article 6: ‘Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal...
data concerning health or sexual life [or criminal convictions], may not be processed automatically unless domestic law provides appropriate safeguards.' The Convention applies to both public sector and private sector organisations. Application to non-automated data is optional.

These are not very high standards for a data protection law to meet. Even so, the ease of compliance is increased by Article 9 which allows derogation from these principles (except the security principle) where

such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; b. protecting the data subject or the rights and freedoms of others.

As Bygrave notes ‘these principles were hardly ground-breaking at the time of the Convention’s adoption’ over 25 years ago. They are even more modest today. Nevertheless, they are a basic set of data privacy principles. The OECD Guidelines are similar but even they are stronger on some points (eg provision of notice; application to non-automated files).

‘European standards’ also requires accession to the Additional Protocol

The Convention neither prevents nor requires data export restrictions to States which are not parties to the Convention and do not have similar data privacy laws, but does allow them under some circumstances (as do the OECD Guidelines). Convention 108 only requires in Article 12 that its parties ‘shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party’. In other words, it guarantees free flow of personal data between parties to the Convention because they have adopted a minimum required standard of data protection. Article 12 also allows restrictions on data exports to other parties in limited circumstances (concerning (a) specific classes of data where the other party does not provide equivalent protection, and (b) where necessary to avoid transfers resulting in onward transfers via a party to a non-party with no similar data protection laws). However, the party wishing to so limit data exports to another party must lodge a derogation to that effect.

The Additional Protocol to Convention 108 in 2001 altered this situation and makes provision for data export restrictions mandatory. Once a party to the Convention also becomes a party to that Protocol, it is required to ‘provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer’ (Article 2 – italics added). The main effect of this provision is that it makes Convention 108 more closely aligned with the EU Directive by adding a data export restriction in similar terms (‘adequate protection’), though expressed in simpler terms. However, by the italicised words, this data export limitation requirement does not apply to transfers to other parties to Convention 108. If they are a party to the Convention, then that is the end of the matter as far as the Convention is concerned (though it might not be the end of the matter for countries bound by the Directive). It is therefore important that the standards for accession be kept high: otherwise parties to the Convention will be forced to allow exports of personal data to countries with low privacy standards.

There are further reasons why it is essential that countries only be allowed to accede to Convention 108 if they also agree to accede to the Additional Protocol. At least in theory it is not necessary for a non-European country to have a data export restriction provision in its law in order to accede to Convention 108. This only becomes necessary if the non-European country wishes to accede to the Additional Protocol. This may have important implications,
because it means that those non-European countries without data export restriction provisions would still obtain the benefit of free flow of personal data from any countries that had also acceded to the Additional Protocol, unless each of those countries lodged a derogation in relation to it under Article 12(3)(b). In other words, data export restrictions are not required as part of the meaning of ‘adequate level of protection’ under Convention 108, even if they are required as part of the Directive’s notion of adequacy.

Concerning enforcement standards, Convention 108 is vague about the sanctions and remedies that the laws of State parties must provide to enforce these principles. It only provides that ‘Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter’ (Article 10). It does add that a person must ‘have a remedy’ of access or correction rights under Article 8, but that does not add anything to Article 10. In short, Convention 108 by itself does not say anything about whether individuals must have a right of individual action to enforce rights, or access to the Courts. It is consistent with it that all enforcement of data protection laws could be by criminal sanctions or administrative remedies. There is no right provided by the Convention of individual complaint against a State party to any Court or other body, so there is no effective method in the Convention itself by which individuals can test whether a party’s implementation of the principles are sufficient, or its enforcement methods are ‘appropriate’ (as required by the Convention). Recourse to the European Court of Human Rights is a separate remedy, but one only available to Europeans.

The Additional Protocol to the Convention also deals with this deficiency by requiring that parties to it ‘shall provide for one or more authorities to be responsible for ensuring compliance’ in its domestic law, and sets out requirements of independence, ability to investigate complaints, to ‘hear claims’, and to bring matters before a Court or to its attention (Article 1). It also requires that the decisions of supervisory authorities ‘may be appealed against through the courts’. It does not require a single data protection authority. These standards would be met by many data protection laws outside Europe, though (for example) Australia’s federal data protection law would currently fall short of this last requirement, as there is no general right of appeal against decisions of the Privacy Commissioner.

From this brief discussion, it should be clear that, taken together, Convention 108 and the Additional Protocol provide a set of standards roughly equivalent to those found in the Directive, and called in this article ‘European standards’, but Convention 108 by itself does not any longer count as ‘European standards’. This is particularly important in relation to the data export requirements. The Council of Europe is at present undertaking a process to ‘modernise’ the Convention. If this ‘modernisation’ were to significantly weaken the standards currently found in the Convention plus Additional Protocol, then this would undermine, and probably make void, most of the arguments presented in the following parts of this article concerning the benefits of non-European accession.

Problems with the procedures and standards for accession

The procedures for accession by non-member states to Convention 108 have not been well-publicised, and even now do not cover all important issues. A September 2011 ‘Note of Information’ on the topic by the Treaty Office of the Council Secretariat (CoE 2011), updating earlier publications, can be paraphrased as follows:

(1) In principle, the Committee of Ministers may take the initiative of inviting a non-member State to accede to a Convention, but it is customary for the non-member
State to request accession in a letter (from their foreign minister) addressed to the Secretary General of the CoE.

(2) Before putting the matter on the Committee agenda, the Secretariat usually informally ascertains opinion among member States’ delegations. For Convention 108, unanimous agreement of all 43 member states who have ratified the Convention (as yet) is required. Formal requests for accession are examined by the Committee or by one of its rapporteur groups.

(3) Once there is an agreement in principle within the Committee to give a positive reply to a request, it instructs the Secretariat to consult the other non-member States which are Parties to the Convention (none as yet), giving them a time-limit for the formulation of objections, usually two months.

(4) In the absence of objections, the decision to invite the non-member State is (usually) taken at the level of the Ministers’ Deputies. The Secretariat General then notifies the State concerned of the invitation to accede to the Convention.

(5) Prior to acceding to Convention 108, the State invited has to take the ‘necessary measures’ to ensure that its domestic law allows the Convention to be implemented (‘to give effect to the basic principles for data protection set out in this chapter’).

(6) The instrument of accession is to be deposited with the CoE in Strasbourg, or delivered by diplomatic courier. The Convention enters into force in relation to the State after three months on the first of the next month.

(7) States are also ‘asked’ to accept the 1999 Amendments to Convention 108 which allowed the European Union to accede to the Convention, as those amendments require unanimous agreement.

(8) Convention 108 has a consultative committee of experts (T-PD) which monitors its application by the States Parties.

While this Note is helpful, it does not address the following five major issues still to be resolved in relation to non-European accessions. All of these must be resolved before the implications of accession for non-European states, and for better global protection of privacy, are clear.

First, the Committee of Ministers needs to determine (or clarify in a public document) that there cannot be non-European accessions except to both the Convention and Additional Protocol, and not just the Convention alone. 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. Allowing accession to the Convention alone will drastically undermine European privacy standards, and is likely to create untenable inconsistencies between the Convention and the Directive. Georges (2011, para 83) refers to ‘the Committee of Ministers’ decision of 2 July 2008 to encourage (non-Member) States having an adequate standard to accede to Convention 108 and its Additional Protocol’, and also assumes in further recommendations to the Consultative Committee that the Convention and the Additional Protocol should be treated as a package. The CoE Secretariat has also advised (personal communication, 5 October 2011) that a requirement to accede to both instruments reflects the Consultative Committee and Secretariat position. It would be important to reflect this key decision in the above Note and in a consolidated publication stating all of these policy
decisions. It appears therefore that this key policy position has been resolved correctly, but it still needs to be stated explicitly in explanatory documents.

Second, the Committee needs to determine the standard by which an assessment is made of whether a country meets the standards for accession to the Convention (and Additional Protocol). The standards for accession are not specified in Article 23, but Article 4 requires that ‘[e]ach Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in [Chapter II of Convention 108]’, by the time of ratification. The ‘Note of Information’ discussed above does not elaborate on what this standard means. It cannot be a merely formal assessment of what a country’s law says on paper. Otherwise, countries like Angola or Malaysia which have laws including a DPA, but have not yet appointed one, would appear to be compliant when in fact they are not. Similarly, India has on paper an apparently strong credit reporting law in force, but it has never been implemented or observed by anyone, including the regulator or the credit bureaus. Because of its previous focus on European accessions, the Convention 108 Consultative Committee has up until now been dealing with ‘normal countries’: democracies in Europe, and all of them within the jurisdiction of the European Court of Human Rights (ECHR). But some of the countries with data privacy laws outside Europe are not ‘normal countries’, and none of them are within the ECHR’s jurisdiction. So the Consultative Committee must exercise extra vigilance to ensure that ‘laws on the books’ are not merely shams. The EU’s approach requiring assessment that a law actually delivers ‘a good level of compliance’, ‘support and help’ and ‘appropriate redress’ must be something close to what should also required for a CoE assessment of what is required for accession.

The standard to the applied should not be exactly the same as that which the EU Commission would apply in determining whether a non-European country’s law was ‘adequate’, but it should be similar in most respects. The key difference is that the Council of Europe should be primarily concerned with how strong is the protection of non-European law from the perspective of the citizens of that country. No particular weight being given to the interests of Europeans, if it is intended that Convention 108 is to become a neutral, global convention. However, when adequacy assessments are made, the Article 29 Committee quite correctly allows more flexibility in the application of the Directive’s standards concerning aspects of a country’s law which are not likely to have any significant influence on the protection of European data subjects (Greenleaf and Bygrave, 2011).

While the standards of the Directive and the Convention should be slightly different, it remains to be seen in practice if Convention 108 accession becomes something of a ‘short cut’ to an EU adequacy finding for non-European countries because it is an ‘international commitment’ that a non-European country has entered and therefore relevant under Article 25 of the Directive. The process might also work in reverse, with the Council of Europe taking into account and giving appropriate weight to a prior adequacy finding for a country (and the WP 29 Opinion on which it is based) when considering requests by non-European states to accede to the Convention and Additional Protocol. But while ‘fast tracking’ of countries that have prior adequacy assessments might be reasonable (Michael, 2008), it should not be automatic. As a practical matter, it would be desirable if the European Commission and the Council of Europe could find a cooperative mechanism by which they could take each other’s findings into account in order to expedite their own. It also remains to be seen whether non-European countries will be satisfied to obtain one or other of an adequacy finding or Convention 108 accession, or whether they will want both.

Third, there needs to be clarification of the procedure which is to be followed by the Council of Europe bodies in making such an assessment, and which parties will be involved. Georges
Greenleaf - The influence of European data privacy standards outside Europe  23

(2011) has proposed to the Consultative Committee detailed procedures by which applications for accession could be assessed, including a major choice of modalities between a 'peer assessment' by representatives of existing member states, or a 'committee of independent experts' with requirements of expertise and independence. However, her recommendations do not fully deal with the question of what 'to give effect to the basic principles' should mean (question 2 above). She does recommend that the Consultative Convention Committee be empowered to give an opinion on conformity when instruments of ratification are deposited or when accession requests are examined by the Committee of Ministers. This would mean it would play a role similar to the Article 29 Working Party under the Directive.

Fourth, and most difficult, is the problem that there is 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 because the European Convention on Human Rights is a closed convention to which non-European states cannot accede (Michael, 2008; Polakiewicz 2011). Perhaps the UN human rights mechanisms for individual 'communications' under ICCPR Article 17 could play a role in relation to non-European countries that are parties to Convention 108 and also to the Optional Protocol under the ICCPR. But that could only apply to some countries. Perhaps the Consultative Committee could be empowered to accept 'communications' from individuals, civil society organisations, or businesses who wish to complain that a party to the Convention is not observing its terms. This would not be comparable to taking a case to the ECHR, but better than nothing. Otherwise, all the Consultative Committee or the Council of Ministers can do is resort to persuasion or public criticism of recalcitrant countries. The answers are not obvious, but they need to be addressed if Convention 108 is to become genuinely global and to give individuals outside Europe genuine means of redress. Otherwise it will remain too biased in favour of the interests of Europeans to be genuinely global. Perhaps the current review of the Convention could take up this issue.

Fifth, there needs to be some procedure to test whether a member state does adhere to its commitments over time, and some sanctions which can be triggered if it does not (somewhat similar to an adequacy assessment being revoked). Georges (2011, para 98) proposes establishment of a periodic review mechanism such as is found in areas like anti-corruption. It is possible that post-ratification assessment of compliance could be dealt with without need for an amendment to the Convention, by such means as a Committee of Ministers' resolution (a separate legal instrument), which non-member states would have to accept upon accession. The current Convention 'modernisation' process, endorsed by the CoE Ministers of Justice in November 2010, has as one of its aims to strengthen the Convention's follow-up mechanism (Polakiewicz 2011), and the interests of non-European states and their citizens need to be kept firmly in mind as part of this process.

All of these issues need to be addressed by the Council's Secretariat in a comprehensive document concerning accession by non-member states if they are to obtain understanding of, and support for, the advantages of accession by the states concerned, and by business and civil society organisations.

The Parliamentary Assembly of the Council of Europe has recently (October 2011) made similar Recommendations to some of the above points: that reform 'should not lower the established protection'; that the Parties should 'establish a mechanism for monitoring compliance'; and that the CoE should encourage ratifications by non-member States (CoE Parliamentary Assembly Recommendation 1984, 2011). The accompanying Resolution makes it clear that 'any global initiative should be based on Convention No 108 and its Additional

**The first example of non-European accession: Uruguay**

At its 1118th meeting on 6 July 2011 the Committee of Ministers under Convention 108 decided to invite Uruguay to accede to the Convention, on the basis of an Opinion provided to it by the Convention’s Consultative Committee, and it is expected it will do so by the end of 2011. The process that led to this decision sheds light on the first three issues discussed above.

The Opinion of the Consultative Committee (CoE TP-D 2011) explains that in this case the delegations of the 43 members of the Consultative Committee (the current parties to the Convention) were provided with Uruguay’s letter requesting accession, its legislation, and the Opinion of the EU’s Article 29 Working Party in relation to Uruguay’s request for a finding of ‘adequacy’ of its law by the EU, which Opinion had been published in 2010 (EU WP29 2010). Fourteen of the 43 delegations replied positively to confirm that in their view Uruguay had taken the necessary measures in its domestic law to give effect to the basic data protection principles of Convention 108 (Bosnia and Herzegovina, Cyprus, the Czech Republic, Estonia, Finland, Hungary, Italy, Latvia, “the former Yugoslav Republic of Macedonia”, Monaco, Slovenia, Sweden, Switzerland and the United Kingdom). No delegation objected. The Consultative Committee then adopted its Opinion supporting accession through written procedure.

The Consultative Committee’s Opinion takes only two pages to detail that Uruguay’s legislation does contain provisions which (on paper) cover all the elements to give effect to the basic data protection principles of Convention 108, but does not directly provide any information to demonstrate that these provisions have any effect in reality or deliver meaningful privacy protection to Uruguayan citizens. However, the Opinion stresses (‘wishes to underline’) the EU WP29 Opinion that found Uruguay’s law adequate. That WP29 Opinion contains 20 pages of detailed analysis of Uruguay’s law and how it satisfies the EU’s requirements, and is based on a much longer expert report obtained by the European Commission and further interaction between the Commission and the Uruguayan government. In particular, concerning the reality of enforcement, the WP29 Opinion says:

"Furthermore, the LPDP [the Uruguayan law], as shown below, includes specific regulations in relation to investigation, inspection and sanctions, and the DPDP establishes specific regulations for certain procedures to be brought before the URCDP [the Uruguayan DPA] and, particularly, for registering processing and authorising international data transfers.

The Working Party wishes to state that evidence has been provided by the URCDP of performance of these powers in a range of information provided during the analysis of data protection adequacy detailed in this document."

A reading of the WP29 Opinion leaves little doubt that, as a matter of reality and not merely of legislative form, Uruguay’s data protection system meets the requirements of Convention 108 and the Additional Protocol. Therefore, although the Consultative Committee Opinion could not in itself be seen to give much reassurance that Uruguay had an effective system of data protection, when taken together with the WP29 Opinion, as was possible in this case, it can be seen to provide sufficient assurance.

If however there are doubts in respect of a candidate for accession, or a lack of information about the real extent of protection, then the Consultative Committee, when requested by the
Committee of Ministers to give an opinion, could appoint members or experts to prepare such an opinion, including by if necessary carrying out a fact-finding mission to the country in question. This has already happened in the past in respect of other CoE conventions, notably in the criminal law field (Polakiewicz 1999, 35-36). Presumably a practice similar to that adopted by the EU could also be followed, where the Commission obtains an expert report and the WP 29 Opinion draws on and refers to that expert report (as it does in its Opinion on New Zealand).

At least the following implications for future assessments of candidates for accession can be drawn provisionally from this first example concerning Uruguay:

(i) The Committee of Ministers will obtain an Opinion from the Consultative Committee (T-PD) (though it is not obliged to), putting T-PD into a position similar to the EU’s Article 29 Working Party.

(ii) EU WP 29 Opinions will be utilised to support a Consultative Committee Opinion.

(iii) The standard applied by the Consultative Committee is not yet clear, but in the case of Uruguay the availability of the WP29 Opinion meant there was assurance that the law did not exist merely on paper, but did provide substantive protection.

(iv) There is no assurance, or requirement, in any of the documentation that Uruguay will adopt the Additional Protocol as part of its accession (issue 1 above), which is a considerable weakness in the process, although probably not as a matter of reality in this instance.

Implications and advantages of accession for non-European states

To summarise the previous discussion, 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). Nor will the resolutions of the meeting of the world’s data protection and privacy commissioners amount to anything by themselves.

Because it has 43 existing members, there are significant advantages for non-European states in acceding 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 Greenleaf 2011). 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 (discussed below).

Advantages for European states in non-European accessions

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. Such a reciprocal obligation can arise if the non-EU country becomes a party to Convention 108. This will soon be a significant advantage to European states.

As the number of countries outside Europe with data privacy laws increases, and those laws include data export limitations (as they almost always do), then in theory European countries (including EU member states) will face the same problems of data export limitations as are faced by non-European countries. How can they be sure that they can import person data from non-European countries without having to comply with a myriad different data export laws in those countries? The simplest and best answer from their point of view will occur when those non-European countries are parties to Convention 108 and the Additional Protocol. Then both countries will have reciprocal obligations of free flow of personal data, and those obligations will also be consistent with the European country’s obligations under the Directive (for those European countries also part of the EU).

5 Conclusions

The first part of this article discusses the geopolitical fact that 29 countries outside Europe have now enacted data privacy laws covering most of their private sectors (and most of those also cover their public sectors), and this growth outside Europe is accelerating. To a surprising extent, these laws share most of the factors that are distinctive of European data privacy laws. The conclusions of this article follow from those two factors.

Globalisation of Convention 108 is possible, but not inevitable

Since there are already 29 data privacy laws outside Europe, with many of them at least having a superficial (ie on paper) strong resemblance to European privacy laws, there would seem to be fertile ground for a significant number of non-European countries to accede to Convention 108. A few would be ruled out by their failure to cover the public sector (Vietnam, Malaysia and India). Laws on paper should not be enough for accession, but a high degree of ‘family resemblance’ does at least suggest a plausible order for the Council of Europe to assess possible candidates for membership (as it has now asked the Venice Commission to do). It can then encourage suitable candidates to apply where it appears that reality might match the law on paper. Convention 108 looks to be at least as promising a candidate for globalisation as the Cybercrime Convention.

Despite this theoretical possibility, there is as yet little of substance to suggest that Convention 108 will become a key instrument of global governance of privacy, despite its great potential to do so. However, it has no realistic competitors as a global privacy instrument. Uruguay is the first country to request to be invited to accede, after its accession received a favourable opinion from the Consultative Committee. The CoE is ‘confident that it
will only be the first country in a long list’ (Polakiewicz, 2011). As yet, the Council of Europe is still doing too little that is public to explain to the rest of the world that that non-European accession to Convention 108 is possible, let alone desirable or with a reasonably transparent procedural mechanism. Its Data Protection Home Page has scattered information on all these matters, but it needs to be consolidated into one convenient location, perhaps under a ‘Globalisation’ heading of equal prominence as ‘Modernisation’. Five key issues that need to be addressed or confirmed have already been discussed above.

Another 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. The CoE has a joint project with ECOWAS to help ensure that the data privacy laws of its member countries meet international standards (Polakiewicz, 2011a). Globalisation of Convention 108 could become one of the most important developments in data privacy over the next decade, but it is too early to tell. It will not happen unless the Council of Europe takes more effective steps to promote the advantages of accession to the rest of the world, and to make its own policies better development and more transparent concerning the standards that must be met for accession, and the procedures to be followed.

This article has stressed the potential advantages of non-European accession to both European and non-European states, and to businesses operating within them. From the perspective of Civil Society (the perspective of this author) the key factor determining whether it will support the globalisation of Convention 108 and the Additional Protocol is that European data privacy standards are not compromised in the process, and that new accessions meet those standards. It is worth repeating that arguments in favour of globalisation are only valid on the assumptions that (i) the current ‘modernisation’ process for Convention 108 does not reduce the privacy standards found in the current Convention plus Additional Protocol, particularly in the key area of data exports; (ii) the non-European accession processes also maintain those standards.

Subject to all these caveats, we should observe that global conventions often take decades to obtain a ‘critical mass’ of ratifications. Convention 108 is well placed to do so by the end of this decade, but there is no inevitability in this result, it will take a lot of determined work.

**Europe should stick to its standards**

The adoption of European data privacy standards in the legislation of a large and increasing number of countries outside Europe is a reason for Europe to adhere to those standards, additional to their intrinsic merit as a statement of human rights. There are no good reasons for Europe to retreat from the privacy standards it has slowly and relatively consistently developed over forty years. There are no alternative global standards worth considering. There are good reasons for European institutions to do a better job of enforcing their own standards, but not for abandoning them.

Increasingly, versions of the European privacy standards are becoming part of the laws of most countries in the world outside Europe (as well as all European countries), as the adoption of new data privacy laws accelerates past the current 78. The significant outliers – principally the USA and China – are few but powerful. They are increasingly living in neighbourhoods of countries that do have data privacy laws. There are some developments within each outlier country sympathetic to effective privacy protection. European and other countries with data privacy laws should continue to put pressure on the businesses and government agencies of these outlier countries, in their international interactions, to comply with what is an increasingly global standard for data privacy. Respect for their domestic
prerogatives should not be confused with any need to reduce fundamental aspects of global data privacy standards.
References


CoE (2011) Council of Europe, Secretariat General, Directorate of Legal Advice and Public International Law (Jurusconsult) Legal Advice Department and Treaty Office Note of Information: Accession to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and to its Additional Protocol regarding supervisory authorities and transborder data flows (ETS No. 181) by States which are not member States of the Council, September 2011 (updating previous publications from at least 1999)


Greenleaf - The influence of European data privacy standards outside Europe


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 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


Montreux Declaration (2005) - The protection of personal data and privacy in a globalised world: a universal right respecting diversities, Declaration of the 27th International Conference of privacy and Data Protection Commissioners, Montreux, Switzerland, September 2005
Greenleaf - The influence of European data privacy standards outside Europe


Polakiewicz, J (2011) ‘Convention 108 as a global privacy standard?’, International Data Protection Conference, Budapest, 17 June 2011 (Head of Human Rights Development Department, Directorate General of Human Rights and Legal Affairs, Council of Europe, but the paper is written in a personal capacity), available from Council of Europe website Data Protection Home Page

Polakiewicz, J (2011a) Opening intervention, International Data Protection Conference, 21 September 2011, Warsaw; available from Council of Europe website Data Protection Home Page


Solove, D The Digital Person New York University Press, 2004


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