2nd & 3rd generation data privacy standards implemented in laws outside Europe

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia
3 July 2017 – *Not to be published - Will be replaced by a shorter abstract*

The implementation of 'European' data privacy principles in laws outside Europe continues to be substantial, but it needs to be defined and quantified in order for its full effect to be understood. This paper will attempt to do so in relation to both the '2nd generation' standards based on the EU data protection Directive (1995) and CoE Convention 108, plus Additional Protocol (2001), and the potential (or 'candidate') 3rd generation standards based on the EU General Data Protection Directive (GDPR) and the 'Modernised' Convention 180.

Defining 2nd generation standards This is shown by the draft Table [TO BE HANDED OUT], an extract from work in progress on the extent to which '2nd generation' data privacy principles/standards are found in data privacy laws in countries outside Europe. The 10 principles/standards in the Table are found in the EU data protection Directive (1995) and CoE Convention 108 + Additional Protocol (2001), but not in the '1st generation' standards of the OECD Guidelines (1980) and original CoE Convention 108 (1981).

In 2012 I assessed[1] 33 of the 39 data privacy laws that then existed outside Europe (as at December 2011) to determine the extent to which they included the ten 2nd Generation' 'European standards'. That analysis showed that they had been substantially incorporated into these 33 non-European laws. On average they included 7 out of the 10 'European principles'. Some occurred in more than 75% of the laws assessed: 'destination-based' data export restrictions (28/33); additional protection for sensitive data (28/33); deletion requirements (28/33); minimum collection (26/33); and two enforcement-related principles (an independent DPA (25/33) and recourse to the courts (26/33)).

Assessing their effect by 2017 By February 2017 the number of non-European laws had increased to 66.[2] Assessment of all 66 countries with data privacy laws, while having the virtue of thoroughness, also has the disadvantage that it treats all countries as of equal weight (as done in the 2012 study). So the data privacy law in Burkina Faso is given the same significance as that in South Africa, and that of a small Caribbean island is given the same weight as that in Argentina. All 66 data privacy laws is also too large a number of laws to be a practical basis for an initial assessment – that task must come later.

For both reasons an objective selection of a particular sub-set of laws outside Europe is needed. An alternative pragmatic approach is to assess the laws of countries with the largest Gross Domestic Product (GDP) (nominal)[3] as a measure of their economic significance. The 20 highest-ranked countries outside Europe that do have data privacy laws covering at least most of their private sectors occur in first 52 countries ranked by GDP.[4] They are, in order of GDP: Japan; India; Canada; South Korea; Australia; Mexico; Indonesia; Argentina; Taiwan; Hong Kong; Israel; the

[1] For the basis of this analysis, see Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2(2) *International Data Privacy Law*, pp. 68–92 <http://papers.ssrn.com/abstract_id=1960299>..

[2] Greenleaf 'Global data privacy laws 2017: 120 national data privacy laws now include Indonesia and Turkey' 145 PLBIR 10-13.

[3] Wikipedia: 'List of countries by GDP (nominal)' <https://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal)>: 'Gross domestic product (GDP) is the market value of all final goods and services from a nation in a given year.' Nominal GDP does not take into account differences in the cost of living in different countries, whereas GDP by purchasing power parity (PPP) does so.

[4] As at 26 February 2017 in Wikipedia: 'List of countries by GDP (nominal)'; The IMF ranking is used instead of the World Bank ranking or the UN ranking beause it includes Hong Kong and Taiwan, but otherwise there is little difference among the three.

Philippines; Malaysia; Singapore; South Africa; Colombia; Chile; Vietnam; Peru; and New Zealand. Their 20 laws are 30% of the 66 laws found at present in countries outside Europe. They include all 8 OECD members outside Europe (except the USA), and 17/20 are APEC economies.

In the Table the principles are sorted by their frequency of occurrence in laws outside Europe, from least often to most often occurring. The data privacy laws of the 'top 20 by GDP' countries outside Europe include on average 5.9 of the 10 2nd generation 'European' standards. The most–implemented principles are the right to seek remedies through the courts (16/20), data deletion (16/20), provision of a DPA (14/20), and restrictions on data exports based at least in part on the laws of the recipient country (14/20). Eight of the 10 principles are included in the laws of at least 11/20 countries, and only two have had relatively little inclusion: limits on automated processing (5/10); and additional restrictions on some sensitive processing, such as prior checking (8/20).

Some of the 20 countries included in the Tables have significant reform Bills in progress. Chile's Bill, if enacted, will include creation of a DPA, and add principles concerning data exports, fair and lawful processing, deletion, and sensitive data. Other legislation is under consideration in Indonesia and New Zealand. If enacted, these Bills will result in the average implementation of principles increasing to greater than 6/10. This 6/10 average is a result not very different from the average of 7/10 inclusions when 33 countries, not restricted to those with high GDP, were assessed in 2012. This suggests that there might only be a modest difference if all 66 countries with data privacy laws are assessed. Effects of European data privacy principles outside Europe continue to be substantial.

Predicting 3rd generation standards The present is a 'watershed period' in the strengthening of content of international agreements. Most obviously, finalization of GDPR and CoE 108 Modernisation signal the development of a new 3rd Generation of European standards. There are as many as 18 new 'candidate standards' in the GDPR, about half of which are included in the Modernised CoE 108. However, the 2013 OECD revision + 2016 APEC revision are also contributing: 5 new standards in GDPR are also found in OECD, most noticeably DBN and Demonstrable Accountability. So the '3rd Generation' will be global standards but with a heavy European influence.

But which of these 18 or so 'candidate standards' will countries outside EU enact? The paper will provide a non-comprehensive set of examples so far of at least 35 of these candidate principles already enacted in countries outside Europe. Which of the 18 'candidates' will become part of the new global 3rd generation of standards will partly depend on such adoption, but also on which principles the EU chooses to make essential for adequacy and which the CoE makes essential for accession.