Is global privacy regulation splintering?

By Blair Stewart, Committee member, Privacy Foundation New Zealand

This article is offered to promote understanding and debate. Opinions expressed are those of the author and not necessarily the Foundation.

Privacy has never had the benefit of a single international standard or treaty or rule setter as is be found in many other areas of law. Instead, the core principles of privacy can be found in, and continue to emerge from, a series of regional and specialist international instruments.[i]

International efforts to seek coherent privacy standards

Although independently promulgated by separate international bodies in processes answerable only to their respective member governments, the principal international instruments on privacy and data protection have not been developed in isolation. Each instrument has been prepared in the knowledge of the others that have gone before. They have influenced each other and together they have created a reasonably coherent whole. This has been facilitated in the last 6 years by revisions of all the major instruments adopted over the previous 35 years.[ii] While there have been differences between the various instruments; the commonalities have been of greater significance.

The coherence of approach can be explained by several factors:

- There has been cross membership of governments across some of the more influential international standard setting bodies active in privacy. For example, a number of European states are members of Council of Europe, European Union and OECD. Non-EU states such as Australia, Canada and USA have been especially influential in the OECD's privacy work.
- Sometimes these national cross-overs result in individuals working in standard setting in more than one forum such as Louis Joinet, from France, who played a key part in the two foundational instruments from the Council of Europe Convention and OECD Guidelines of 1980 as well as the lesser known United Nations General Assembly instrument of 1995.[iii] (Closer to home, the author was honoured to be part of the experts' group that revised the 1980 OECD Guidelines[iv] and also to have led the working group within APEC's Data Privacy Subgroup that revised the 2005 APEC Guidelines in 2014[v].)
- A recognition by governments and international policy makers that in the absence of a global treaty it is in everyone's interests that the regional and specialist instruments can work in harmony. This is partly driven by philosophy but also by the practical needs of enforcement bodies and of businesses that operate across regional borders or globally. In 2013 the OECD explicitly adopted a policy of encouraging the development of international arrangements that promote interoperability between privacy frameworks. This objective of interoperability was endorsed by APEC in 2015.

These international bodies have been motivated to be active in privacy standard setting for various reasons including, in some cases, concern for the protection of human rights of their citizens. A principal driver has been to facilitate international trade and promote economic growth. The needs of global companies and businesses trading in multiple jurisdictions have been a particular concern. While coverage of the world by national privacy laws remains somewhat patchy[vi] the international standard setters have had some success in seeking to promote a degree of consistency in approach in order to avoid undue barriers to global commerce that might have arisen from incompatible regulations. Looked

at in prosaic terms, the objective would be to enable a global company to adopt a single worldwide policy for personal information handling that would be compliant in all jurisdictions.

Thus far this note has told, in briefest outline, a simple story in terms of the development of international privacy instruments and the progress in achieving a central core of privacy principles in approximately the same terms within a range of privacy instruments emanating from quite diverse bodies. However, it appears that this reasonably rosy picture of progress may be starting to unravel.

Splintering of international privacy standards

In this last part of the note I highlight a few examples that might perhaps point towards a trend that undermining both the apparent consensus amongst policymakers that a free flow of information in a seamless and inter-connected internet is desirable and the tendency of global business to operate a single global privacy policy that seeks to meet the legal requirements of individuals in all regions, even though such an approach may exceed what is legally required in some places. I refer to this as 'splintering' in two senses: (1) splintering of a single recognisable set of core privacy standards into requirements that differ in important respects between regions, and (2) global companies departing from universality and delivering quite different privacy rights to people in different regions.

The issues cannot of course be divorced from the internet given that cross-border business involving consumers is likely to involve the internet. Although my focus is solely in relation to privacy regulation, the splintering of unified regulatory approaches to support a seamlessly interconnected internet is by no means limited to this sphere. Indeed, some of the quite substantial differences in approaches to, say, censorship and social control, may perhaps lead to splits in the internet. The term 'splinternet' has been coined which Wikipedia explains as follows:

> The **splinternet** (also referred to as cyber-balkanization, cyber-balkanisation, internet balkanization, or internet balkanisation) is a characterization of the Internet as splintering and dividing due to various factors, such as technology, commerce, politics, nationalism, religion, and interests. 'Powerful forces are threatening to balkanise it', writes the *Economist* weekly, and it may soon splinter along geographic and commercial boundaries. Countries such as China have erected what is termed a 'Great Firewall', for political reasons, while other nations, such as the US and Australia, discuss plans to create a similar firewall to block child pornography or weapon-making instructions.

One might suggest that data export controls such as contained in the EU Directive of 1995 contribute to splintering but I not in the sense I am using in this note. Those controls were crafted around the privacy principles generally recognised internationally since 1980 with the long-term aim of supporting free flow of data by promoting trust.

Instead, I would see the emergence of data localisation laws as one of the early counter trends to the acceptance of a general core set of accepted privacy principles as the accepted basis for doing global information business.[vii] These data localisation laws require that personal information about a nations' citizens or residents be collected, processed, and/or stored inside the country. Wikipedia explains:

> **Data localization** builds upon the concept of data sovereignty that regulates certain data types by the laws applicable to the data subject or processor. While data sovereignty may require that records about a nation's citizens or residents follow its personal or financial data processing laws, data localization goes a step further in requiring that initial collection, processing, and storage occur first within the national boundaries. In some cases, data about a nation's citizens or residents must also be deleted from foreign systems before being removed from systems in the data subject's nation.

One spur to data localisation laws was national security concerns about US Government practices resulting from the Edward Snowden revelations (2013) although there have been examples since at least

2004 when British Columbia took this course for medical records (also prompted by concerns at US information practices).

One attempt in our region to counter any emerging trend towards data localisation requirements is found in the Comprehensive and Progressive Trans Pacific Partnership. The CPTPP establishes a restriction on data localisation requirements in article 14.13: "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."[viii] This general restriction is subject to at least three exceptions: government data, financial services and a general four-step test exception.[ix]

The next prominent example of a splintering of international privacy standards has been the emergence of the privacy principle usually called the 'right to be forgotten'. In a 2014 judgment, the European Court of Justice concluded that this right existed in the 1995 EU Data Protection Directive. Although it may not be that unusual for national constitutional courts to discern new rights as part of interpreting 'living laws' to meet the needs of society it was somewhat unexpected in the context of trans-national laws governing data protection. The impact of the judgment went well beyond the EU since its first impact was to be felt by US search engine companies.

The significance of the right as an example of 'splintering' results from its emergence from case law rather than policy formulation. It was therefore not subject to the usual policy processes, nor have full legislative flexibility, to promote the benefits of a free flow of information and international interoperability as well as to accommodate the prosaic business impacts. (As an aside, the right was later included in the law that replaced the 1995 Directive following normal policy processes – including intensive business lobbying - in that instance resulting in a narrower 'right to erasure'.)

The splintering that this right illustrates is two-fold:

- The right was not to be found in any other international instrument and so marked a departure from the consensus core privacy standards. However, this point should not be overstated since establishment of a new standard does not of itself necessarily represent serious splintering: any extension of privacy rights has to start somewhere and could eventually be picked up in other instruments as happened with the emergence of privacy breach notification which emerged first in the USA before being adopted reasonably quickly into all the principal international instruments.[x]
- More significantly, the global search engine companies implemented the new privacy right solely for EU countries. While that might at first seem unsurprising given the remit of EU law the practice of global companies differentiating their privacy compliance practices in this way departs from the maxim of operating a single global information management policy based upon the strictest data protection requirements. While one can certainly understand US companies not operating the right in the US if they think it is contrary to their local constitutional requirements should the US approach govern their privacy practices in non-US countries?

The final example of splintering is the new EU right to data portability. Like the right to be forgotten (right to erasure), this right does not feature in any of the other international instruments. Unlike that other right there is no US first Amendment issue at stake. The splintering issue is whether global companies are going to extend this right in a universal fashion to everyone. It's too early to say for sure

but the likelihood is that global companies won't volunteer to share data in a way that makes it easier for consumers to shift to a competitor. Nor is there any indication yet that other regional standards are likely to pick up this important new right.

What impact for New Zealand of any splintering of global privacy standards?

New Zealand is a small remote country dependent upon international trade. Our people are great travelers and users of global networks. As with many areas of regulation, our interests are best served by effective multilateral standard setting into which our interests are taken into account.

Given the absence of a global privacy standard, New Zealanders' privacy interests are probably most usefully protected served by a strong local privacy law coupled elsewhere with a broad spread of well enforced and interoperable foreign privacy laws. However, if the laws in different regions are not aligned to standards that are interoperable we are left vulnerable to international business practices. Up until now we have benefited from global business aligning to the strictest standard which has been the EU Directive and now GDPR. However, if global businesses get a taste for doing privacy well in the EU but dropping to low US standards elsewhere where does that leave us?

In terms of trade, as a general proposition it also seems undesirable for NZ businesses operating globally to be faced with an environment in which other countries erect barriers in the form of data localisation laws. Our companies will lose some access to those markets: the CPTPP is one protection against that trend. It will also be harder for our companies, which are more likely to be SMEs than large multi-nationals, to trade internationally if global standards drift apart.

It seems likely to be detrimental to New Zealanders if global companies move further away from attempting to adhere to the most stringent privacy standards globally to a position where they apply strong EU protections only in the EU and treat the rest of the world to low US standards as a default.

Blair Stewart, Auckland, 14 May 2019

[i] The principal international privacy instruments for the purpose of this note were adopted by the OECD in 1980 (updated 2013), Council of Europe in 1981 (updated 2018), European Community/European Union in 1995 (updated/replaced 2016) and APEC in 2005 (updated 2015).

[ii] APEC has been quite explicit in acknowledging that it used the OECD Privacy Guidelines of 1980 as the 'starting point' in developing its 2005 Privacy Framework. Similarly, the revision of the APEC Framework completed in 2015 explicitly drew upon the changes made by the OECD in 2013.

[iii] An interesting short account illustrating the contributions of individuals in developing the 1980 OECD Guidelines, and the cross-cutting influences of numerous international bodies into that OECD work, can be found in Michael Kirby's presentation to a roundtable on the 30th Anniversary of the guidelines. See: http://www.oecd.org/internet/ieconomy/44945835.doc

[iv] See, for instance, outline and papers from OECD Workshop, "30 Years After: The Impact of the OECD Privacy Guidelines", Paris, 2010: http://www.oecd.org/internet/ieconomy/30yearsaftertheimpactoftheoecdprivacyguidelines.htm

[v] See APEC Privacy Framework Stocktake: Comparative Review Against 2013 Updates to OECD Guidelines (Narrative), Data Privacy Subgroup meeting, Subic Philippines, 1 February 2015: http://mddb.apec.org/Documents/2015/ECSG/DPS1/15_ecsg_dps1_006.pdf

[vi] Of the approximately 195 countries in the world, apparently about 132 now have privacy laws. See Graham Greenleaf: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380794

[vii] See Courtney Bowman, Data Localization Laws: An Emerging Global Trend, 2017 https://www.jurist.org/commentary/2017/01/courtney-bowman-data-localization/

[viii] https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf

[ix] See Michael Geist, Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards, 2018 https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security

[x] The GDPR right to erasure - the regulatory right which has in effect since 2016 codified the right to be forgotten - might eventually be reflected in the core set privacy rights across other regions. Unfortunately for that prospect the timing of the 2014 judgment meant that it emerged too late to be an influence in the updates of either the OECD or APEC instruments.