International data privacy agreements after the GDPR and Schrems

Greenleaf, Graham

30 January 2016

(2016) 139 Privacy Laws & Business International Report 12-15

[2016] UNSWLRS 29

International data privacy agreements after the GDPR and *Schrems*

Graham Greenleaf,* Professor of Law & Information Systems, UNSW Australia

(2016) 139 *Privacy Laws & Business International Report* 12-15

30 January 2016

Contents

* Valuable information for and/or comments on for this article were received from Blair Stewart, Marie Georges, Sophie Kwasny and Jörg Polakiewicz. Responsibility for all content remains with the author.

Now that the content of the EU's General Data Protection Regulation (GDPR) has substantially been settled, and the *Schrems* decision of the European Court of Justice has confirmed the parameters within which both it and the existing EU data protection Directive of 1995 must be considered, what are the implications for international agreements affecting data privacy? Also, what is the evolving landscape of international agreements to which these developments contribute? This brief article aims to sketch the larger picture, not to fill in all the details.

Council of Europe Convention 108 – The emerging global agreement

Council of Europe (CoE) data protection Convention 108 of 1981 (with its Additional Protocol of 2001) is strengthening its position as the emerging global data privacy agreement, but there remain unresolved issues in its operation.

EU and CoE – more in tandem

A quiet development with long-term significance is that the European Union is now more strongly supporting Convention 108 as a global privacy treaty. At the same time as it finalised the terms of the GDPR, the Council of the EU adopted as one of its priorities for 2016-7 in its relationships with the CoE 'Finalisation of the works on the modernisation of the Council of Europe Convention on data protection (Convention 108) with a view to the EU joining the convention' and to 'Support the worldwide promotion of this Convention.'[1]

Consistent with this development, a late addition to the draft text of the Preamble to the GDPR states that when the Commission, in making adequacy decisions, is taking into account a third country's international commitments, 'In particular the third country's accession to [CoE Convention 108] should be taken into account' (clause 81a). This is a clear signal to all non-European countries interested in obtaining EU adequacy assessments that they should consider a prior or concurrent application to accede to Convention 108.

These EU developments have significant implications for both the globalisation and the modernisation of Convention 108.

Globalisation – accessions expand, procedures are incomplete

The Consultative Committee on Convention 108 (known as T-PD) has provided its opinions on three new applications by non-European countries that wish to accede to the Convention and its Additional Protocol: Mauritius, Senegal, and Tunisia, resulting in three new invitations to accede in 2015.[2] Such invitations are valid for five years from when issued.

In each case the Consultative Committee Opinion carefully compares the constitutional provisions and the data privacy legislation in the candidate countries with the provisions of Convention 108 and the Additional Protocol, and finds that their laws do meet these requirements sufficient for it to recommend that an invitation to accede be issued by the Committee of Ministers (or their Deputies). For Senegal it found they were met 'in general' and did not recommend any amendments. For Mauritius it found they were met 'on the whole', but only recommended that Mauritius 'engage in the future to put in line with the provisions of the Convention' issues raised in the Opinion, but did not require specific amendments (and nor did the invitation decision). For Tunisia, the Opinion found that their law 'generally heads toward the principles giving effect' to the Convention and Protocol, but

[1] Council of the European Union, Political and Security Committee – 1/A Item Note to Permanent Representatives Committee/Council 'EU priorities for cooperation with the Council of Europe in 2016-2017', Brussels, 15 December 2015, COSCE 7 CFSP/PESC 831 COHOM 121. 'The Committee invites the Council, subject to approval by the Permanent Representatives, to adopt the priorities in the Annex', one of which was Item 2.3 Rule of Law b. 'Data protection', as quoted above.

[2] Consultative Committee 'Opinion on the request for accession of Mauritius' 18 December 2014, T-PD (2014)10 (Invitation to accede issued 1 April 2015); 'Opinion on the request for accession of Senegal' 22 May 2015, T-PD(2015)05 (Invitation to accede issued 1 July 2015); 'Opinion on the request for accession of Tunisia' 15 October 2015, T-PD(2015)14 (Invitation to accede issued 2 December 2015).

that 'several modifications are necessary to bring it into full conformity, and recommends that the Committee of Ministers invites [Tunisia] to accede to both instruments, once it has complied with the observations set out above.' However, the invitation decision by the Committee of Ministers was unconditional, and did not mention any of these 'necessary' modifications. We can expect that the T-PD Chair and Secretariat have close relationships with the Tunisian authorities, and have obtained assurances that these modifications will be carried out before accession. But an unconditional invitation gives the appearance that an Opinion from the Consultative Committee is being ignored by the Committee of Ministers, and raises unnecessary questions about maintenance of Convention standards. If it is not possible for the Secretariat to include some informal explanation when Committee of Ministers' decisions are issued, then perhaps the Committee should reconsider its approach.

It seems to be clearly in the interests of all parties that there is a high degree of consistency between EU adequacy decisions and CoE accession invitations. The need for this will be even stronger under the GDPR and the modernised Convention. At present, the procedures of the two organisations are very different, with risks of different outcomes. EU adequacy assessments require an intensive investigation (usually initially through an 'Expert Report' to the Commission) which looks at all aspects of how a candidate country's laws are administered and enforced, and what privacy-protective results they deliver.

A problem with the existing Convention 108 is its 'conditions of membership' only requires a Party to 'take the necessary measures in its domestic law to give effect' to the principles in the Convention. (Article 4). The requirements for accession by non-European States (Article 23) add nothing more except the unanimous vote of existing Parties. The view is therefore taken that the Consultative Committee has no mandate to evaluate anything beyond the 'law on the books' of candidate members. As a result, the Consultative Committee procedures do not (insofar as is revealed by its Opinions) involve basic checks, such as the number of staff and budget of the DPA, and whether its website or annual report discloses active investigation or other means of enforcement. Perhaps these checks are in fact done, but this is not apparent from the Opinions, for the above reason.

The reciprocal nature of Convention 108 obligations make it crucial for the confidence of both existing and prospective member States that the standards of adherence to the Convention be at a high level, and transparently so.[3] The 'modernised' Convention 108 will remedy the current deficiencies. The duties of Parties will be not only to enact laws applying the Convention, but also to 'secure their effective application' (Article 4). The Consultative Committee (renamed as 'Convention Committee') will, in relation to any proposed accession, provide an opinion on 'the level of personal data protection' of the candidate member, and recommended measures to reach compliance with Convention requirements (Article 19(e)). This wording aligns closely with the EU's terminology concerning adequacy assessments. Furthermore, the Convention Committee 'shall review the implementation of this Convention by the Parties and recommend measures to take where a party is not in compliance' (Article 19(h)). This will apply to existing Convention parties, making this similar to the 'period review' of adequacy assessments which will be required by the GDPR (discussed below).

Modernisation – final steps

With the EU's completion of the GDPR, a committee (called CAHDATA) of State representatives, plus Observers must complete the 'modernisation' of the text of a revised Convention 108, in light of the final GDPR text. There is no expectation that the revised Convention 108 will include data protection standards as strong as the GDPR, but it must require Convention parties to at least provide protection which the EU would consider 'adequate' under the GDPR. Otherwise, the EU's endorsement of Convention 108 would make little sense. It is likely that the Secretariat of Convention 108 will

[3] This argument is expanded in Graham Greenleaf 'The UN Special Rapporteur: Advancing a Global Privacy Treaty?' (2015) 136 *Privacy Laws & Business International Report*, 7-9.

prepare new draft terms of reference for a CAHDATA meeting, for approval by the Committee of Ministers, and invitations then sent to delegations, probably for a meeting to be held in May 2016. Given that finalization of Convention 108 is now a priority of the EU, prior to it joining the Convention, the EU delegation can be expected to play an active role in CAHDATA's deliberations.

European Union – Past, present and future overlap

While all eyes are on the GDPR, the 1995 Directive still has some years of life left in it – as recent decisions of the European Court of Justice have shown. If the GDPR is adopted early in 2016, as expected, it will come into force two years later in 2018, and at that point replace the Directive. However, interpretation of the relationships between the Directive and the GDPR, express and implied, will be complex for many years to come.

Still life – EU Directive 1995-2018

Although 'adequate' is no longer quite as definitive as it was thought to be, more countries are seeking positive adequacy assessments under the existing Directive. In April 2015, Japan's government announced in the Diet that it would seek an adequacy assessment as soon as it passed its reform Bill (now enacted).[4] In December, the Korean government issued a press release that it was seeking an adequacy assessment.[5] Other than for India's failed attempts, these are the first known attempts to obtain adequacy assessments by Asian countries. Whether either of them will also seek to accede to CoE Convention 108 is not known. In light of *Schrems*, the standard that Korea or Japan will have to meet is that of 'essential equivalence' to EU law,[6] a standard arguably more strict than was previously applied.

Countries that obtain an adequacy assessment under the Directive will still be considered adequate under the GDPR (GDPR Article 41(8)) … for a while. However, the EU Commission will be required by the GDPR (Article 41) to conduct a 'periodic review, at least every four years' of all adequacy assessments (old and new), taking into account all relevant developments in the country and in international organisations (which developments are also to be monitored continuously), and may repeal, suspend or amend adequacy decisions. All existing adequacy decisions will therefore be reviewed, and according to the stricter adequacy standards of the GDPR (and *Schrems*). 'Grandfathering', but perhaps a very grumpy grandad in some undeserving cases.

In recent years, the EU has already started doing some reviews of existing adequacy applications – most obvious with previous Safe Harbor reviews, but also occurring in less contentious cases such as New Zealand[7] – but they were not required, nor to a timetable, as in the GDPR.

GDPR – generational change?

The final GDPR compromise text was not a case of 'To Infinity and Beyond', but more like a small step for mankind: a more modest set of advances than many proposals from the Commission and the Parliament during the past five years had suggested. The 1995 Directive signalled the arrival of a '2nd Generation' of data privacy standards that have had great influence outside Europe for two decades,

---

[4] Hiroshi Miyashita 'Japan amends its DP Act in light of Big Data and data transfers' (2015) 137 *Privacy Laws and Business International Report*, 8-11.

[5] News release from Ministry of Information (MOI), Korea, 15 December 2015, stating that the Korean government will seek an EU adequacy assessment to assist Korean businesses in transactions with EU member states, and will proceed to amend Korea's legislation, if necessary.

[6] *Schrems v Data Protection Commissioner*, para. 73: 'the term "adequate level of protection" must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.'

[7] Blair Stewart 'Update on NZ's 'Adequacy' under the EU Data Protection Directive' *NZ Commissioner's Blog*, 24 December 2015 <https://privacy.org.nz/blog/update-on-nzs-adequacy-under-the-eu-data-protection-directive/>

to the extent that the current global standard of privacy protection is closer to the Directive than to the OECD Guidelines.[8]

An important global question concerning the GDPR is to ask which of its new content principles and enforcement requirements are likely to become standard elements of data privacy laws outside the EU: a '3rd Generation' of evolving global data privacy standards. Within Europe this will be influenced (but not fully determined) by which new GDPR elements become in substance part of the modernised Convention 108. Outside Europe, a mixture of the influence of perceived 'adequacy' requirements in the GDPR, what is required for Convention 108 accession, and desire to emulate European 'best practices' will be influential. And it must not be forgotten that some of the 'new' GDPR elements have already been enacted outside the EU (or included in the 2013 revised OECD Guidelines), and are therefore inherently global, not European.

The result will take some time to become clear, but the list of candidates for '3rd Generation' standards (after more detailed consideration) includes the following:

1. *Rights apply to all data subjects*, irrespective of nationality/residence;
2. *Stronger consent requirements* – including 'unambiguous' and unbundling requirements;
3. *Right to portability of user-generated content (UGC)*;
4. *Right to erasure/ 'to be forgotten'*;
5. *Mandatory Data Protection Officers (DPOs) for sensitive processing*;
6. *Mandatory Data Protection Impact Assessments (DPIAs) for high risk processing*;
7. *Data protection by design and by default*;
8. *Direct liability for processors* as well as controllers;
9. *Foreign controllers must be represented within the jurisdiction*;
10. *Data breach notification* to both DPA and if high risk to data subjects;
11. *Class actions by public interest privacy groups*;
12. *Maximum fines based on global annual turnover*;
13. *DPAs are to make decisions and issue administrative sanctions*;
14. *Right of judicial appeal against DPA decisions*;
15. *DPAs must cooperate in resolving complaints with international elements*;
16. *Demonstrable accountability required of data controllers*.

All of these candidates are found in the GDPR and/or the draft modernised Convention 108, and in a couple of cases the 2013 OECD Guidelines revision. Some can be said to be implied by the 1995 Directive (arguably including 1, 7 and 9 above), but have now been made more explicit and are therefore included in the above list. Hindsight will reveal that not all of these will become part of new global standards (through adoption in national laws outside the EU), but many will.

EU Free Trade Agreements (FTAs)

The EU is negotiating what it describes as 'a trade and investment deal with the US', the Transatlantic Trade and Investment Partnership (TTIP),[9] and various other FTAs such as one with India. Although the final decisions are made by the States of the EU and the European Parliament, the European Commission can 'negotiate' concerning data protection provisions in FTAs. However, it can only do so within the parameters of, and according to the procedures of, Article 25 of the EU data protection Directive, as interpreted in *Schrems*.

The Council of the EU confirmed in December 2015 that the Commission cannot negotiate away privacy rights in trade agreements: 'The Council stresses the need to create a global level playing field in the area of digital trade and strongly supports the Commission's intention to pursue this goal *in full*

[8] For justification of this conclusion, see Greenleaf, G 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' *International Data Privacy Law*, Vol. 2, Issue 2, 2012 < http://ssrn.com/abstract=1960299>; and G Greenleaf Asian Data Privacy Laws (OUP, 2014), Chapter 17.

[9] EU Commission's TTIP pages <http://ec.europa.eu/trade/policy/in-focus/ttip/documents-and-events/index_en.htm>

compliance with and without prejudice to the EU's data protection and data privacy rules, which are not negotiated in or affected by trade agreements'[10] (emphasis added).

Unlike with most other FTAs, the EU's negotiating position on the TTIP is disclosed,[11] following disquiet with secret negotiations,[12] and is much the same as in GATS Art XIV(c)(ii), to which the member countries of the WTO are already committed. However, it may also aim to obtain more substantive guarantees of privacy protections in US law than the TPP requires. If the EU maintains such approaches in the TTIP negotiations (and in other FTA negotiations), it will be providing a less privacy-hostile alternative for FTA development than has emerged from the Trans-Pacific Partnership (TPP) text.[13]

Depending on what the EU negotiates, this may have even more direct benefits for Australia, because of a 'side letter' to the TPP between Australia and the US providing that 'Should the Government of the United States of America undertake any relevant additional commitments to those in the TPP Agreement with respect to the treatment of personal information of foreign nationals in another free trade agreement, it shall extend any such commitments to Australia.'[14] According to Michael Geist, Canada did not obtain such a TPP concession from the US.[15]

EU (and some other) citizens suing in the USA

The US *Judicial Redress Act* 'authorizes the Department of Justice (DOJ) to designate foreign countries or regional economic integration organizations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain U0S government agencies for purposes of accessing, amending, or redressing unlawful disclosures of records transferred from a foreign country to the United States to prevent, investigate, detect, or prosecute criminal offenses.' [16] It is part of a package of measures designed to address the problems of EU to US personal data transfers, made more acute by the *Schrems* decision, passed the House of Representatives in October. The Senate Judicial Committee on 28 January forwarded the Bill to the full Senate, but added extra complicating conditions. The US-Australia TPP 'side letter' referred to above also provides that the US 'will also endeavour to apply extensions of privacy protections with respect to personal information of foreign nationals held by the United States Government to Australian citizens and permanent residents.' Apparently Canada has not extracted any such concessions, so not all TPP parties have done so. US negotiators are masters of 'divide and conquer', and the arts of forum-shifting to achieve their ends.

Safe Harbor 2.0 may invite Schrems 2.0

On 2 February 2016, EU Justice Commissioner Jourová announced the completion of negotiations for the optimistically-titled 'EU-US Privacy Shield', otherwise known as 'Safe Harbor 2.0'. The details, which cannot be analysed here, will be incorporated in an 'adequacy decision' to be finalised through EU processes in the following weeks, while the US finalised arrangements on its side.[17] In doing so, one of the Commission's required tasks will be (as the ECJ summarised it in *Schrems*[18]) 'to find that the

---

[10] Council of the European Union *3430th Council meeting OUTCOME OF THE COUNCIL MEETING Brussels, 27 November 2015* December 2015 <http://www.consilium.europa.eu/en/meetings/fac/2015/11/st14688_en15_pdf/>

[11] The EU's position in the negotiations <http://ec.europa.eu/trade/policy/in-focus/ttip/documents-and-events/index_en.htm#eu-position>

[12] 'Decision of the European Ombudsman closing the inquiry into complaint 119/2015/PHP on the European Commission's handling of a request for public access to documents related to TTIP' <http://www.ombudsman.europa.eu/en/cases/decision.faces/en/61261/html.bookmark>

[13] Greenleaf, G 'The TPP Agreement: An anti-privacy treaty for most of APEC' (2015) 138 *Privacy Laws & Business International Report,* 1, 3-7.

[14] US-Australia side letter, undated <https://ustr.gov/sites/default/files/TPP-Final-Text-US-AU-Letter-Exchange-on-Privacy.pdf>

[15] Michael Geist 'The Trouble with the TPP, Day 14: No U.S. Assurances for Canada on Privacy' michaelgeist.ca Blog, 21 January 2016 <http://www.michaelgeist.ca/2016/01/the-trouble-with-the-tpp-day-14-no-u-s-assurances-for-canada-on-privacy/>

[16] Summary of House Bill 1428 < https://www.congress.gov/bill/114th-congress/house-bill/1428>

[17] European Commission Press Release Database 'Speaking points by Justice Commissioner Jourová at the press conference on the new framework for transatlantic data flows: the EU-US Privacy Shield' 2 February 2016 <http://europa.eu/rapid/press-release_SPEECH-16-221_en.htm?locale=en>

[18] Court of Justice of the European Union, Press Release No 117/15 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid', 6 October 2015 <http://curia.europa.eu/jcms/jcms/P_180250/>

United States in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the directive read in the light of the Charter.' The Commission must make such a finding in relation to the content of Safe Harbor 2.0, and do so convincingly, or it will be inviting *Schrems* 2.0 in due course.

APEC's privacy instruments

APEC is considering proposed reforms to the 2004 APEC Privacy Framework, proposed by its Privacy Sub-group. The proposals are essentially to align the Framework with the 2013 amendments to the OECD privacy Guidelines, in such matters as accountability, breach notification, Privacy by Design and privacy metrics. Adoption of the changes was not completed in 2015, but may be in early 2016.

APEC's Cross-border Privacy Rules system (CBPRs) is still struggling to get started. After nearly a decade, it has until 2016 had only has one functioning member country (the US) with an Accountability Agent (AA), TRUSTe, which has a compromised reputation[19]). In January 2016 APEC announced that it had approved an AA for Japan, a 'trustmark' provider, JIPDEC,[20] which also derives its funds from accreditations and has little reputation for enforcement.[21] Only two other countries (Mexico and Canada) have started but not completed the membership process. APEC CBPRs currently means little more than a potential means to facilitate personal data transfers from other countries to the US. Japan's entry only means that companies in Japan that sign up to APEC CBPRs with JIPDEC will be able to claim to be 'APEC compliant', but whether this will assist any companies in other countries to transfer personal data to Japan remains to be seen. JIPDEC's approval as an AA is for one year.

APEC added during 2015 a method of recognising processors ('Privacy Recognition for Processors' - PRP) within the CBPRs.[22] APEC states that "The PRP helps personal information processors ("processors") demonstrate their ability to provide effective implementation of a personal information controller's ("controller") privacy obligations related to the processing of personal information. The PRP also helps controllers identify qualified and accountable processors." At present, this would only be relevant to processors located in the US.

The latest 'APEC privacy instrument' (significantly, minus China) is the Trans-Pacific Partnership (TPP), which aims to prevent data export limitations and data localization provisions.[23]

Other international developments

The UN Special Rapporteur on the right to privacy,[24] Joseph Cannataci has kept a low profile since his appointment in July 2015.[25] There is as yet little public indication of how he will shape his three year role, other than a sketch of a 10 point plan to guide his work to a closed session of the Data Protection Commissioners Conference in October 2015.[26] Concrete progress has not yet been made on international standards for limitation of mass surveillance, but may emerge from the work of the

---

[19] Connolly, C, Greenleaf, G and Waters N 'Privacy self-regulation in crisis?: TRUSTe's 'deceptive' practices' (2014) 132 *Privacy Laws & Business International Report,* 19-21.

[20] Advice from the APEC Secretariat to APEC ECSG (Electronic Commerce Steering Group) members, 19 January.

[21] Graham Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 261-63.

[22] APEC ECSG *APEC Privacy Recognition for Processors (PRP) - Purpose and Background* 28 August 2015, Forum Doc. No.: 2015/SOM1/021anx5a <http://mddb.apec.org/Documents/2015/ECSG/DPS2/15_ecsg_dps2_007.pdf>

[23] Graham Greenleaf ''The TPP Agreement: An anti-privacy treaty for most of APEC' (2015) 138 *Privacy Laws & Business International Report,* 1, 3-7.

[24] Special Rapporteur on the right to privacy, web page, Office of the High Commissioner for Human Rights <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

[25] Graham Greenleaf 'The UN Special Rapporteur: Advancing a Global Privacy Treaty?' (2015) 136 Privacy Laws & Business International Report, 7-9.

[26] There is bullet point summary in 'Closed session welcomes UN Special Rapporteur on the Right to Privacy' (2015) 1(7) *ICDPPC Newsletter*, November 2015 <https://icdppc.org/wp-content/uploads/2015/11/ICDPPC-Newsletter-–-Volume-1-Edition-7-–-Special-edition-November-2015.pdf>

Rapporteur and the Civil Society 'necessary and proportionate' initiative to develop principles on communications surveillance.[27]

The African Union's *Convention on Cyber-security and Personal Data Protection* has disappeared from view since its adoption by the AU in June 2014.[28] It is not even listed on the AU's website for treaty status lists.[29] No signatures, let alone ratifications, are known. The 15 ratifications needed for the Convention to come into force seem a long way off. However, 2016 is the African Year of Human Rights, so perhaps it will be an *annus mirabilis* as well.[30]

Conclusion – A Great Game continues

Post GDPR, the most important influences in the global development of privacy standards remain European (both EU and Council of Europe), even though European jurisdictions are now the minority of those with data privacy laws. The most significant challenge to this legal hegemony continues to come from the United States, both from its ability to shape the Free Trade Agreements that threaten to cripple data export restrictions, and from the global ubiquity and economic power of those of its businesses based on the exploitation of personal data. When they can bring personal data within the 'safe harbor' of the US, they are able to act with relative impunity in relation to the laws of other countries. This game has now been playing for nearly 40 years, and both sides are again refreshing their tactics, and checking who is on their team.

---

[27] *International Principles on the Application of Human Rights to Communications Surveillance* <https://en.necessaryandproportionate.org/>

[28] Graham Greenleaf and Marie Georges 'The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?' (2014) 131 *Privacy Laws & Business International Report*, 18-21

[29] OAU/AU Treaties, Conventions, Protocols & Charters <http://www.au.int/en/treaties>

[30] *Annus Mirabilis* is a poem written by John Dryden, published in 1667, commemorating 1665–1666, the 'year of miracles' of London (Wikipedia).