University of New South Wales Law Research Series

IT'S NEARLY 2020, SO WHAT FATE AWAITS THE 1980 OECD PRIVACY GUIDELINES?

GRAHAM GREENLEAF

(2019) 159 *Privacy Laws & Business International Report* 18
[2019] *UNSWLRS* 42

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

It's nearly 2020, so what fate awaits the 1980 OECD privacy Guidelines?

(A background paper for the 2019 OECD privacy Guidelines review)

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

I have prepared this Background Paper to assist my work as a member of the OECD's Privacy Guidelines Expert Group (PGEG), which provides advice to the Working Party on Security and Privacy in the Digital Economy (SPDE), and to assist and encourage informed debate on the significance of reform of the Guidelines. Comments are welcome. A shorter version of this paper is published in (2019) 159 Privacy Laws & Business International Report 18-21.

10 June 2019

Abstract: The Organisation for Economic Co-operation and Development (OECD) is again reviewing, and perhaps revising, its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* originally made in 1980, and revised once in 2013. It is therefore an opportune time to consider what continuing relevance do the Guidelines have, and what are the prospects of this review making them more relevant to the future of data privacy laws. This background paper surveys the origins and significance of the 1980 Guidelines and their very limited revision in 2013. It is unclear whether the 2019 'review' which is now underway will be a further revision. 1980 is nearly 40 years ago, and the international environment now includes the GDPR, Convention 108+, and regional instruments and standards which are much stronger than the Guidelines.

The overall question addressed in this paper is whether the Guidelines will serve a useful future purpose if they are not revised and strengthened substantially. They could remain largely as they are, a bastion of low privacy standards. Or they could be revised to become a moderate (rather than rock-bottom) minimum standard of data privacy protections, and as a more credible candidate for what convergence initiatives could aim to implement.

* Valuable comments have been received from Marc Rotenberg, Elizabeth Coombs, and others unnamed, but all responsibility for content remains with the author. This paper is based in part on updated extracts from G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), Chapters 2 and 19.

[1] See OECD 'OECD work on privacy' <http://www.oecd.org/sti/ieconomy/privacy.htm> - The review is mentioned but

The Organisation for Economic Co-operation and Development (OECD) is again reviewing, and perhaps revising,[1] its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[2] ('the Guidelines'), originally made in 1980, and revised once before in 2013. It is therefore an opportune time to consider what continuing relevance do the Guidelines have, and what are the prospects of this review making them more relevant to the future of data privacy laws.

The OECD is an intergovernmental organization which now has 36 member countries, [3] 27 of which are from Europe, and plans for enlargement.[4] All OECD members (other than the USA in relation to the private sector), now have comprehensive data privacy laws implementing the Guidelines. They were developed simultaneously with the Council of Europe's data protection Convention 108 of 1981, with considerable interaction between the committees developing each instrument,[5] and have very considerable overlap in their principles with Convention 108. Together, the Guidelines and Convention 108 comprise the 'first generation' of international data privacy standards.

This background paper surveys the origins and significance of the 1980 Guidelines, their very limited revision in 2013, and the 2019 'review' which is now underway but it is not clear whether it is another revision. 1980 is nearly 40 years ago, and the international environment now includes the GDPR, Convention 108+, and regional instruments and standards in Africa and Latin America which are much stronger than the Guidelines. The overall question addressed here is whether the Guidelines will serve a useful future purpose if they are not revised and strengthened substantially.

1. The Guidelines of 1980 – Form, content, influence and deficiencies

The Guidelines of 1980 were one of the earliest formulations of a comprehensive set of information privacy principles. They are in the form of a Recommendation by the Council of the OECD. Unlike Decisions, Recommendations of the Council are not legally binding on member states. The Guidelines are proposed as minimum standards for the protection of privacy and individual liberties. They attempt to balance two 'essential basic values': the protection of privacy and individual liberties and the advancement of free flows of personal

---

[1] See OECD 'OECD work on privacy' <http://www.oecd.org/sti/ieconomy/privacy.htm> - The review is mentioned but no documentation is yet public.

[2] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, Paris, 1981), adopted as a Recommendation of the Council of the OECD, 23 September 1980.

3 List of OECD Member Countries (OECD, 2013) http://www.oecd.org/general/listofoecdmembercountries-ratificationoftheconventionontheoecd.htm: Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israël, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. The European Commission is entitled to take part in the work of the OECD.

[4] Discussions concerning membership by Brazil and Argentina are said to be in progress. In 2007, OECD countries agreed to invite Chile, Estonia, Israel, and Slovenia to open membership discussions (all have since become members), but Russia, also invited, has not. OECD offered enhanced engagement, but not membership, to Brazil, China, India, Indonesia and South Africa' (OECD website).

[5] OECD Guidelines Explanatory Memorandum, para. 20: 'the Expert Group maintained close contacts with corresponding organs of the Council of Europe'; M. Kirby 'Privacy today: Something old, something new, something borrowed, something blue' (2017) 25(1) Journal of Law, Information and Science 1; [2017] JlLawInfoSci 1 <http://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html>; Kirby notes that European experts central to the OECD Guidelines were also very involved in Council of Europe and EU data protection initiatives.

data.[6] They apply to both the public and private sectors. As early as 1999 they were criticized as an inadequate standard,[7] including by the chair of the committee that drafted them.[8]

The core of the Guidelines are the eight 'basic principles of national application' in Part Two (principles 7–14). These are principles concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. The Guidelines contain four 'basic principles of international application' concerning the free flow of personal data, and legitimate restrictions on such data exports (principles 15–18). The main thrust of these four principles is that member countries should avoid restrictions on the free flow of personal data among themselves, coupled with the recognition that restrictions on data exports can be legitimate, as set out in three exceptions in Guideline 17, the first of which is where the other member country 'does not yet substantially observe these Guidelines'. The implementation requirements of the OECD Guidelines are minimal. Paragraph 19 states the methods of implementation required for compliance with the Guidelines, but they only amount to encouragement to member states to adopt whatever mix of legislation and self-regulation they consider appropriate, provided that they deliver 'reasonable means for individuals to exercise their rights', 'adequate sanctions and remedies' and 'no unfair discrimination against data subjects'.

The Guidelines were developed by an Expert Group chaired by Justice M.D. Kirby, then Chairman of the Australian Law Reform Commission. In a 2017 retrospective[9] he explains the interplay of personalities and ideologies involved in the drafting of the Guidelines. He argues that the US achieved 'what it had been primarily seeking', which was that the Guidelines would not be a binding instrument, and the recommendation that member countries should 'endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data'. 'The Europeans, led by France', on the other hand, 'gained an American endorsement of the then gold standard of the European principles, around which would soon be clustered national laws for the protection of information privacy in most OECD countries'.[10]

Influence of the 1980 Guidelines

The Guidelines were initially influential, particularly in encouraging the adoption of data privacy laws in at least eight countries outside Europe, mainly in the Asia-Pacific[11] (they were not needed in Europe because of Convention 108). However, from around 1995 when the EU's data protection Directive was adopted, implementing a higher standard of data protection than the Guidelines, their influence started to wane. Non-European countries (and non-EU countries in Europe), whether or not OECD members, increasingly saw the EU Directive as the

[6] 'While accepting certain restrictions to free trans-border flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.'

[7] For example, see Roger Clarke, 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (unpublished, 2000) <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html>. This very detailed critique 'catalogues the deficiencies that were inherent in the "fair information practices" tradition that the OECD's 1980 Guidelines codified, together with the additional problems that have arisen since their formulation'.

[8] Michael Kirby, 'Privacy protection, a new beginning: OECD principles 20 years on' (1999) 6 PLPR 25.

[9] Kirby 'Privacy today: Something old, something new…'

[10] ibid, p. 12.

[11] Non-European countries enacting data privacy laws from 1980 up to 1995 (when the EU Directive was made) are: Israel; Canada; Australia; New Zealand; South Korea; Hong Kong SAR; Taiwan; and Japan.

global 'international best practice' for emulation, and some also aspired to obtain an 'adequacy' finding from the EU for their own levels of protection.[12]

The influence of the Guidelines has not been solely in terms of the number of countries that formally adhere to them and enact accordingly, but also their influence as a standard to which non-member countries may aspire. Because of their overlap with Convention 108, all of the OECD principles are included in the EU's data protection Directive, which adopted and extended the content of Convention 108. The Guidelines had very substantial influence on the APEC Privacy Framework, which is based closely on them, but whether the APEC Framework has had much influence on any national laws is debatable.[13] The exact influence of the Guidelines, as distinct from that of Convention 108 and the EU Directive, is therefore almost impossible to determine, but there is nothing to be gained by denying that the original 1980 version of the Guidelines had significant influence, mainly outside Europe, for at least a decade and a half.

Deficiencies of the 1980 Guidelines

By 1995, the inadequacy of the Guidelines to provide sufficient privacy regulation in a world about to enter the Internet era was most clearly seen in the key elements which were required by the EU data protection Directive, but were not required by the Guidelines (or by the original version of Convention 108). The ten most important such differences arguably[14] are:

1. **Minimum necessary collection** for the purpose of processing (not simply 'limited');
2. A general requirement, and exhaustive definition, of **'legitimate processing'**;
3. **Prior notification to or** checking by DPA for some processing;
4. **Data retention limits** (destruction or anonymisation) after processing achieved;
5. Additional protections for particular categories of **sensitive data**;
6. Limits on **automated decision-making**, and a right to know its logic;
7. Requirement to provide **'opt-out' from direct marketing, and other rights to object;**
8. Requirement of an **independent Data Protection Authority** (DPA);
9. Requirement of **recourse to the courts** to enforce data privacy rights;
10. Requirement of **restrictions on personal data exports** based on whether recipient country provided adequate protection (or other sufficient protections).

The Directive's innovations, combined with the 'first generation' (Convention 108/OECD) standards, constituted the second generation of international data privacy standards. Largely adopted by Convention 108, they are reasonably described as 'European standards'.[15]

Almost 25 years later, any of these ten elements look unsurprising as components of a data privacy law. In fact laws enacted in countries outside Europe (now more than 70 of the 134

[12] Argentina, Canada, Israel, Uruguay and New Zealand (and some smaller jurisdictions) succeeded in doing so under the Directive, and Japan has done so under the GDPR. India and Australia, and probably other jurisdictions, tried but failed to do so.

[13] G. Greenleaf Asian Data Privacy Laws (OUP, 2014), pp. 36-7.

[14] G. 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>.

[15] The 10 elements, except 3, 6 and 7, were also part of Convention 108 once it added its Additional Protocol in 2001.

countries with such laws) include on average approximately seven of the ten[16] or probably even higher if non-EU European laws are included. This gap between what the OECD Guidelines require and both what 'European standards' require, and the reality of what is actually enacted, is still the clearest measure of how far short of the current global data privacy standard the OECD Guidelines now fall. The GDPR, Convention 108+, and laws influenced by them now being enacted, are widening this gap further.

2. Revised OECD privacy Guidelines 2013

From 2011–13 an expert group including non-government experts, convened by the OECD's Working Party on Information Security and Privacy (WPISP), and chaired by Canada's then Privacy Commissioner, considered the revision of the Guidelines and prepared a report.[17] 'On the basis of the work by the expert group, proposed revisions were developed by the WPISP and approved by the Committee for Information, Computer and Communications Policy (ICCP), before final adoption by the OECD Council'[18] of the 2013 Guidelines and Supplementary Explanatory Memorandum.[19] The final revisions were therefore a matter of intergovernmental negotiation, and matters on which the expert group had little say. Last-minute changes to both the Guidelines and the Memorandum, which weakened them substantially, were such that one involved expert described it as a 'procedural hijack'.[20]

The revised Guidelines do not change the core 'Principles of National Application' at all from the 1980 version (described above), but did add some useful new content on implementation, plus some new weaknesses (see below). However, it is difficult to see much significance in the 2013 revision if all it does is preserve a standard that almost every OECD member already exceeded. One answer is that the 2013 Guidelines were aimed at least as much at countries that are not OECD members, partly so as to limit the extent that they can implement restrictions on data exports. These changes are now explained.

The frozen OECD principles—A wasted opportunity

The Expert Group proposed that the eight Basic Principles of National Application in Part Two of the 1980 Guidelines should be unchanged, not because they were regarded by participants as satisfactory, but because 'no clear direction emerged as to what changes might be needed', meaning that there was no possibility of obtaining consensus within the expert group.[21] The OECD's privacy principles therefore remain frozen at 1980 levels, as if nothing (including the EU data protection Directive) had occurred in the intervening 33 years. Even though this may have been strategically necessary, in order to salvage even the 1980 principles, this result

[16] Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe' (2012); see also G. Greenleaf, ''European' Data Privacy Standards Implemented in Laws Outside Europe' (2017) 149 *Privacy Laws & Business International Report* 21-23 < https://ssrn.com/abstract=3096314>

[17] *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines* (OECD, 11 October 2013) <http://www.oecd-ilibrary.org/science-and-technology/privacy-expert-group-report-on-the-review-of-the-1980-oecd-privacy-guidelines_5k3xz5zmj2mx-en>.

[18] 'OECD work on privacy' (OECD, 2013) <http://www.oecd.org/sti/ieconomy/privacy.htm>.

[19] *2013 OECD Privacy Guidelines and Supplementary Explanatory Memorandum* (OECD, 2013) <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>. The 2013 Guidelines and the 'OECD Cross-border privacy law enforcement cooperation' have also been re-badged as the 'OECD Privacy Framework': *The OECD Privacy Framework* (OECD, 2013) <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>.

[20] Nigel Waters, 'Hijacked: The revised OECD Privacy Guidelines (2013)' (2013) 125 *Privacy Laws & Business International Report*, p. 13.

[21] Some of these divisions, involving proposals to both strengthen and weaken the 1980 Principles, are indicated indirectly by the 'issues identified for possible further study' in the expert group report; *Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines* (2013), pp. 8–11.

ignored the fact that the overwhelming majority of the 101 data privacy laws enacted globally by 2013[22] embodied considerably higher data privacy standards than the 1980 Guidelines.[23]

The principles in the OECD Guidelines (1980 and 2013 versions) now represent little more than the maximum that the USA will accept in an international agreement, at least so long as the USA fails to enact in its own comprehensive data protection law. Even the idea that there should be some time limit on how long personal data is held was deferred by the OECD for further study,[24] despite being a common feature of almost all data privacy laws for the last 30 years.[25] Omission of most of the other distinctive elements of the Directive now looks similarly antiquated.

Stronger aspects of the 2013 Guidelines

The 2013 Guidelines are in four significant respects stronger than the 1980 Guidelines, particularly in relation to enforcement, moving them slightly closer to global standards for data privacy laws. A new Part Three, 'Implementing Accountability', includes requirements of a 'privacy management programme' with specific requirements, including that data controllers should be prepared to demonstrate the programme, particularly to enforcement bodies. Whether this is 'accountability without liability' needs clarification.[26] Mandatory data security breach notification is also recommended, to enforcement authorities, and to data subjects where they are likely to be affected. These changes can be seen as reinforcing the OECD's 'accountability' and 'security' principles, and also as strengthening enforcement.

The 2013 Guidelines also add recommendations that countries should establish 'privacy enforcement authorities' with sufficient resources and expertise to exercise their powers effectively and make impartial decisions (but without requiring 'independence', as European standards require). It is also recommended that countries should 'make public the details of their observance' of the Guidelines and 'encourage the development of internationally comparable metrics', and the explanatory materials clarify that this includes publication of complaint statistics and similar matters than can improve policy-making, particularly if done in internationally consistent fashion.[27]

Failed 'globalization' of the Guidelines—An attempt to weaken data export restrictions?

The 1980 Guidelines could be adopted only by OECD member countries, and they only attempted to regulate relationships between OECD members, a small group of economically advanced countries. The 2013 Recommendation by the Council 'invites non-Members to adhere to this Recommendation and to collaborate with Member countries in its implementation across borders'. Given this Recommendation, it would seem that any references to a 'Member country' in the text of the Guidelines should be read as a reference to

---

[22] G. Greenleaf, 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories', (2014) 23(1) *Journal of Law, Information & Science* <http://www.jlisjournal.org/abstracts/greenleaf.23.1.html >; also at <http://ssrn.com/abstract=2280877>.

[23] G. 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>.

[24] Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines, pp. 8–11.

[25] Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe'.

[26] G Greenleaf 'Accountability without liability: 'to whom' and 'with what consequences'?' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3384427>.

[27] The matters discussed here are in pt. 5 'National Implementation' and pt. 6'International Co-operation and Interoperability'.

'an adhering country' whether or not a member, otherwise adherence would mean nothing.[28] Any country can now adhere to the Guidelines by a simple declaration.

This is the first and obvious sense of 'globalisation' of the Guideline. If it had been successful, it would have enabled them to be more effectively promoted as one of the alternative global privacy standards. However, it has been a failure: no non-member has been known to have publicly announced it would adhere to the Guidelines in five years 2013-18, and no new laws are known that implement only the OECD's principles. There is no obvious benefit to any non-member in announcing adherence to the Guidelines. It could hypothetically be argued that there is some benefit in encouraging countries without data privacy laws to adopt such laws to a consistent minimum standard, but no country would look to the OECD Guidelines as that standard any longer. In any event, this globalisation is a failure.

However, the attempted 'globalisation' also has potential dangers. The 2013 Guidelines attempt, though a series of subtle steps, to limit the extent to which any countries that endorse the Guidelines (whether OECD members or not) can then impose limitations on data exports to any other countries.[29] At the same time, these steps also convert what was previously a 'minimum standards' agreement between OECD members into something closer to 'maximum standards' in relation to data export restrictions.[30] These effects continue to apply to OECD members, but as these are only guidelines, and they contradict both the GDPR and Convention 108, their influence on many if not all OECD members will be limited. The most likely dangers would have arisen with countries that have not yet adopted data privacy laws.

---

[28] This is because all Guidelines are framed in terms of the obligations of 'Member countries'.

[29] Once a country (OECD member or not) has adhered to the 2013 Guidelines, the 'Basic Principles of International Application' require that an adhering country 'should refrain from restricting transborder flows of personal data between itself and another country' where one of two conditions are met. The reference to 'another country' (meaning any other country in the world) is in itself a major change, because the 1980 Guidelines only imposed restrictions on data flows between member countries, leaving OECD countries free to do what they liked in relation to other countries. This is the second sense in which the 2013 OECD Guidelines are 'globalized'.

There are two conditions (in article 17) that may prevent any further restriction of data exports if either is satisfied by any other country which has announced its adherence to the Guidelines: '(a) the other country substantially observes these Guidelines' (but that 'observance' need not, according to the Guidelines, be by legislation) or '(b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines'. Requirement (b) in effect rules out any export restricts based solely on the destination of a data export, and requires that other types of safeguards (e.g. binding corporate rules, standard contract clauses) must be allowed. This is not necessarily very different from what is required by article 26 of the EU data protection Directive (or the revised Convention 108); the important thing is that it will apply to any country adhering to the Guidelines.

[30] A difficult question, on which they Guidelines are ambiguous (see below), is whether adhering countries can impose conditions on data exports where they consider special protection is needed, such as in relation to classes of sensitive data, or exports for the purpose of particularly sensitive types of processing. If the restrictive interpretation is correct (which is not certain), the upshot of these changes is that any country adhering to the Guidelines (OECD member or not) must allow data exports to any other country adhering to the Guidelines (OECD member or not) on the basis set out in article 17 and no more restrictive.

The 2013 Guidelines still say in art. 6 that they 'should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties'. How is this consistent with the apparent maximum standards allowed by art. 17? The phrase 'which may impact transborder flows of personal data' has been added to art. 6, and it appears from the Supplementary Explanatory Memorandum that the intention is to confirm that 'additional measures' under art. 6 can also result in additional restrictions on transborder flows under art.17, but this is uncertain and the position is still somewhat ambiguous. In any event, any restrictions on data exports, including additional measures, also have to comply with the Guidelines that they 'should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing'.

None of these aspects of 'globalization' of the 2013 Guidelines are mentioned in the Supplementary Explanatory Memorandum, and are generally not remarked upon by other commentators. Nevertheless, some of them deserve to be reversed.

Other changes that weaken the Guidelines

The 1980 Guidelines required members to 'take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure'. This is completely removed from the 2013 Guidelines, which in light of the Snowden revelations is a very convenient result for many OECD member governments, and a very poor result for other countries and their citizens.

Although the 2013 Guidelines say explicitly that member countries 'should … adopt laws protecting privacy', this is not as straightforward as it sounds. It is arguable that the Guidelines as a whole, weaken the importance of implementation by legislation, in favour of non-legislative approaches.[31] However, these are only non-binding Guidelines, so it is also possible that legal hair-splitting about terminology is less important than the apparent encouragement of legislation.

Influence of the 2013 Guidelines

The changes to the 2013 Guidelines that strengthen them (data breach notification, demonstrable accountability etc), may have had a positive effect on reform of existing laws in OECD member countries outside Europe. Since 2013, countries such as Australia and Canada have enacted data breach notification laws, and others such as Singapore and Malaysia propose to do so. However, such laws were already part of the European Commission's GDPR agenda as early as 2010,[32] so the OECD Guidelines cannot take sole credit for their popularity. The EU's adoption of an expanded 'demonstrable accountability' principle also dates from WP29's 'Accountability Opinion' of 2010.[33] Like the 1980 Guidelines, the strengthened aspects of the 2013 Guidelines has operated in concert with European developments, has helped create the minimum standards largely common to privacy laws across the world.

However, just as the 1980 Guidelines did not result in much uniformity in approaches to data exports, effects of the ambiguous provisions in the 2013 Guidelines have not been observable. 'Improving interoperability among privacy frameworks' has effectively become a goal of the Guidelines through inclusion in its recitals, as well as being one of the guidelines, [34]giving a clear indication of the agenda of some OECD members, most clearly the USA. The overall result is that the OECD Guidelines are playing an increasingly political role, as the flagship for a lower global standard of privacy protection, and as an opponent of data export restrictions.

---

[31] The 1980 Guidelines included in the Recommendations by the Council 'that Member countries take into account in their domestic legislation' the Guidelines, and in the Guideline concerning national implementation, that they 'endeavour to … adopt appropriate domestic legislation' to implement them. However, the 2013 Guidelines drop all of this, with the Council now only recommending that member countries 'implement the Guidelines … through processes that include all relevant stakeholders', and the Guideline concerning national implementation includes in a list of non-legislative measures, 'adopt laws protecting privacy', which have been defined more broadly than specific data protection laws. What this adds up to is that the Guidelines no longer require a commitment to enact data protection legislation implementing the Guidelines. Approaches such as APEC's CBPR, or a scattering of laws such as in the USA, can be more easily argued to suffice.

[32] Greenleaf, Graham, Global Data Privacy in a Networked World (October 14, 2011). *Research Handbook on Governance of the Internet*, I. Brown, ed., Edward Elgar, 2012, p. 242; <https://ssrn.com/abstract=1954296>

[33] ibid, p. 240.

[34] Article 21 says countries should support developments that 'promote interoperability among privacy frameworks that give practical effect to these Guidelines'.

3. The 2019 review – or revision?

In November 2018 the OECD Secretariat outlined the process for another review of the Guidelines, to result in a report to the OECD Council by the Working Party on Security and Privacy in the Digital Economy (WP-SPDE).[35] Six months later, no details of this process or its objectives are available to the public, other than an acknowledgment that '[i]n 2019 the OECD is working with countries and experts to scope developments and provide practical recommendations on the implementation of the Guidelines in today's digital environment'.[36] Key questions include whether the process is intended as a revision of the 2013 Guidelines, or merely a review of their implementation. The Secretariat has convened a Privacy Guidelines Expert Group (PGEG) of over 60 participants, which has held a series of conference calls in early 2019. Whether members of the PGEG are arguing for a genuine revision of principles of the Guidelines is also not public.

Therefore, whether the 2019 review process, and the Guidelines, should be regarded as worthless is not something on which the public can yet form a view. However, it is a debate which is of public importance, and it should not occur completely behind closed doors. More transparency is needed from the OECD.

A more balanced process?

A notable positive feature of previous OECD work on privacy has been the attempt to ensure there is meaningful Civil Society input into many OECD activities, in addition to government and business input. In 2008 at the OECD Seoul Ministerial the Civil Society Information Society Advisory Council (CSISAC)[37] was established, and had significant engagement in the 2013 revision of the Guidelines, though not with results to its satisfaction.

The first WP-SPED Consultation, on Accountability, in this process is not reassuring in terms of Civil Society involvement, with only about 5 of 90 participants (and 3 of 15 speakers) being from Civil Society, whereas there were 25 business representatives involved. The PGEG group of experts is more balanced, with over 20% of participants from Civil Society (including academics). The OECD Secretariat should aim for higher Civil Society participation in the Guidelines review.

4. Future value of the Guidelines: Convergence or irrelevance?

The changed international environment for privacy post-GDPR leaves the OECD with a choice. The choice depends to a significant extent on what approach the US decides to take.

One option is to leave the Guidelines as they are, ignoring almost all of the stronger rights for data subjects, and stronger obligations on controllers and processors, becoming common in many of the data privacy laws already enacted in 134 countries. This might be coupled, as in 2013, with adding a few stronger implementation features, and some more restrictions on data export limitations or data localisation.[38] From one perspective, this would amount to

---

[35] OECD Secretariat *Process for the review of the OECD Privacy Guidelines* Working Party on Security and Privacy in the Digital Economy, OECD, 15 November 2018.

[36] See OECD 'OECD work on privacy' <http://www.oecd.org/sti/ieconomy/privacy.htm>..

[37] Civil Society Information Society Advisory Council (CSISAC) website https://csisac.org/: 'We facilitate the exchange of information between the OECD and civil society participants …'

[38] These are the current priorities of US data privacy policies, as seen in the TPP (now the CPTPP, unchanged on these points despite the departure of the US), and the (unratified) USMCA free trade agreement: Greenleaf, Graham, Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108 (November 30, 2018). (2018) 156 *Privacy Laws & Business International Report* 22-24.

'weaponising' the Guidelines (and the APEC instruments that follow their lead) as a continuing bastion of low privacy standards. On other perspectives, this would make them largely irrelevant to the future.

The other option, even if it is coupled with leaving Part Two untouched (as in 2013), is to add a considerable range of new rights and obligations reflecting some of the content of the GDPR and Convention 108+, thus positioning the OECD Guidelines as a more credible contender to be a moderate (rather than rock-bottom) minimum standard of data privacy protections, and as a candidate for what convergence (or even 'interoperability') initiatives could aim to implement. Whether this option will appeal to the US probably depends on whether it moves to adopt a Federal data privacy law, and therefore becomes interested in negotiating a future position for US interests, rather than defending a now-untenable position of the past.