University of New South Wales Law Research Series

ACCOUNTABILITY WITHOUT LIABILITY: 'TO WHOM' AND 'WITH WHAT CONSEQUENCES'? (QUESTIONS FOR THE 2019 OECD PRIVACY GUIDELINES REVIEW)

GRAHAM GREENLEAF

[2019] *UNSWLRS* 67

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

Accountability without liability: 'to whom' and 'with what consequences'?

(Questions for the 2019 OECD privacy Guidelines review)

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

6 May 2019

This paper is the Speaking Notes for my presentation at the OECD Expert Consultation on Accountability, held at the OECD, Paris, on 6 May 2019. I am 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). Some detailed citations appropriate for a published article have been omitted. Comments are welcome, to assist future revision for publication.

Abstract

The concept of accountability, though present in international data protection agreements since the 1980s, has gained more prominence since its elaboration in the 2013 revision of the OECD privacy Guidelines and the 2016 EU *General Data Protection Regulation* (GDPR). In the GDPR art. 24 'demonstrable accountability' has become an additional and separate obligation on data controllers. If a controller fails to so demonstrate compliance, the supervisory authority can order it to bring its processing operations into compliance, and/or impose an administrative fine. The GDPR implementation can be described as 'accountability with liability'.

The wording of the 2013 revisions of the OECD Guidelines new Part Three 'Implementing Accountability' leaves a number of matters ambiguous that would benefit from clarification in the revision of the Guidelines, so as to move from 'accountability without liability', to 'accountability with liability'. This paper proposes three revisions.

APEC (Asia Pacific Economic Cooperation)'s Cross-border Privacy Rules system (CBPRs), is regarded as a leading non-legislative implementations of 'accountability', including in the 2013 revision of the Guidelines. I argue that it is a very unsuccessful implementation, which should not be followed, nor promoted by the Guidelines. There are three main reasons:

- After being in operation for seven years, only two countries – the USA and Japan – participate fully, in that they have nominated an AA and that AA certifies companies. Even the participation of these two countries should be classified as a failure, since on 24 US companies have been certified since 2013, and 3 Japanese companies since 2015.

- There are a few aspects of the operation of APEC's CBPRs (removal of certification, referrals to PEAs, and anonymised case notes) which go directly to the questions of whether either its Accountability Agents (AAs), or the companies they certify, really are 'accountable' in the sense of having any liability for failure to comply with CBPRs rules. Despite six years as the USA's AA, TrustArc's web pages do not contain any information at all about any of these matters.

- The potential for 'interoperability' between CBPRs and other international instruments concerning data protection, is mentioned in Background Papers and the Guidelines themselves. The Guidelines are too low a standard to suit this purpose, as the EU has recognized in it adequacy decision concerning Japan.

In conclusion, five recommendations are made to address accountability gaps in the OECD Privacy Guidelines, including removal of misleading references to APEC CBPRs.

Contents

The concept of accountability, though present in international data protection agreements since the 1980s, has gained more prominence since its elaboration in the 2013 revision of the OECD privacy Guidelines and the 2016 EU *General Data Protection Regulation* (GDPR).

Although 'accountability' has five main usages (transparency, liability, controllability, responsibility, and responsiveness), [1] three of these (transparency, liability, and responsiveness) imply that accountability is to some third party, and all five raise the question of what are the consequences of not providing this form of accountability.

It is therefore worth asking whether the accountability found in the revised OECD Guidelines deals with both accountability 'to whom' and 'with what consequences'? These two aspects are most clearly present in accountability considered as liability. It is vital that they be unambiguous whenever accountability is to be implemented through legislation.

1. Accountability with liability: EU GDPR

The EU's 2016 *General Data Protection Regulation* (GDPR), art. 24 ('Responsibility of the controller') is the clearest implementation in legislation of accountability as liability. It provides that controllers '*shall* implement appropriate technical and organisational measures to ensure and to *be able to demonstrate* that processing is performed in accordance with this Regulation.' Re-stating this, art. 5(2) provides that the controller 'shall be responsible for, and able to demonstrate compliance with' the principles relating to the processing of personal data' in art. 5(1), which it labels 'accountability'. The expression 'demonstrable accountability' is in common use in relation to the GDPR.[2]

Therefore, in addition to being required to implement measures to ensure that processing is in fact performed in accordance with the GDPR, the controller must also be able to demonstrate such compliance. If a controller fails to so demonstrate compliance, the supervisory authority can order it to bring its processing operations into compliance, and/or impose an administrative fine (art. 58(2)(d) and (i)).

---

[1] Christopher Docksey 'Article 24 – Responsibility of the controller' in C. Kuner, L. Bygrave, and C. Docksey *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP, 2019, forthcoming); Docksey cites Koppell, 'Pathologies of Accountability' 65(1) Public Administration Review (2005) 1994.

[2] The 'modernised' Convention 108 ('108+') also includes a brief version of this obligation in art. 8bis.

'Demonstrable accountability' therefore becomes an additional and separate obligation on data controllers. As Christoper Docksey puts it: 'the proactive obligation to adopt appropriate measures and the obligation to be able to demonstrate compliance are new obligations which, quite apart from any failure to respect applicable accountability-related obligations, would in themselves render controllers liable for non-compliance'.[3] What Docksey refers to as 'the link between accountability and sanctions' was made by WP29 in 2010, when it said that 'when and if data controllers fail to fulfil the accountability principle, there is a need for meaningful sanctions', and Docksey adds 'this is in addition to the actual infringement of substantive data protection principles.'[4] The GDPR implementation can be described as 'accountability with liability'.

2. Accountability without liability?: OECD guidelines

The 1980 OECD Guidelines version of accountability is brief: 'A data controller should be accountable for complying with measures which give effect to the principles stated above'. This does not make clear to whom such an obligation is owed, if anyone. It also does not make clear that this is an obligation which can be breached, and carry consequences for breach, in the same way as other Principles in Part Two of the Guidelines.

The 2013 revisions of the Guidelines adds Part Three 'Implementing Accountability' which expands considerably the meaning of 'accountability' in the Guidelines. The whole of Part Three (cl. 15) is preceded by 'a data controller should' (followed by (a) Have in place a privacy management programme that …; (b) Be prepared to demonstrate …; and (c) Provide notice …).

This wording leaves a number of matters ambiguous that would benefit from clarification in the revision of the Guidelines:

1. It should be made clear that when a country adopts laws protecting privacy (cl. 19(b)), the protections provided in Part Three should be give the same status as those in Part Two, in relation to all of the national implementation mechanisms in Part Five (enforceability, means of enforcing rights, sanctions and remedies etc). In a large proportion (possibly a majority) of the 134 national data privacy laws around the world, and in state laws in the USA, data breach notification (cl. 15(c)) has similar enforcement mechanisms as do other privacy principles.

2. The same should be the case with the obligations to implement and demonstrate a privacy management programme (PMP) (cl 15(b) and (c)), as occurs with the GDPR and its separately enforceable obligation of 'demonstrable accountability;.

3. The question of 'accountable to whom' is addressed, but not explicitly enough. In cl. 15(b) a privacy enforcement authority (PEA) is able to request demonstration of a PMP, 'request' should be replaced by 'requirement'. In cl. 15(c) the situations when notice must be provided to a PEA, and when to data subject, are stated clearly, but it also needs to be stated that these parties can seek remedies if data controllers fail to give the required notice. It is not stated or implied to whom the obligation to have in place a PMP is owed (PEA and/or data subjects and representatives who can act on their behalf), and that they can require such a PMP to be put in place, and to seek remedies for failure by the data controller to do so.

[3] ibid

[4] ibid

The 2013 version of the OECD Guidelines can be interpreted as 'accountability without liability', and should be modified to ensure that they exemplify 'accountability with liability'.

CIPL's 'Accountability Wheel' does not include any clear statement of the element of liability, although it purports to map all comprehensive data protection laws 'including the GDPR'.[5] The statement that the GDPR adopts the CIPL concept of accountability, and other 'global privacy laws should follow suit'[6] is therefore unsupportable and should not be adopted until it is modified to clarify that it refers to accountability with liability.

3. APEC's Framework and CBPRs

APEC (Asia Pacific Economic Cooperation), its Privacy Framework, and its Cross-border Privacy Rules system (CBPRs), are all established by means other than treaties or legislation, and so are regarded as non-legislative implementations of 'accountability'. I argue that they are very unsuccessful implementations, which should not be followed, and which should not be considered as a possible basis for any form of 'interoperability'.

APEC's Privacy Framework (2004, revised 2015): A weakened implementation

The APEC Privacy Framework (2004, revised version 2015), which is simply another set of guidelines (and APEC has no basis in any treaty), provides the same wording as the OECD accountability principle (para. 14): 'A personal information controller should be accountable for complying with measures that give effect to the Principles stated above' (para. 32).

However, APEC adds 'When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.' This appears to be an attempt to substitute a form of accountability principle for a principle limiting data exports. It provides some basis in the APEC Privacy Framework for the APEC Cross-border Privacy Rules system (APEC CBPRs). However, if the recipient does not in fact protect the information, the data subject is left unprotected: 'accountability', but no liability on any party.

The revised APEC Privacy Framework includes in Part III 'Privacy Management Programmes' in terms similar to, but not identical with, the 2013 OECD Guidelines Part Three 'Implementing Accountability'. As well as many differences in wording, there are differences in substance which make the APEC version weaker than the OECD version. Instead of 'a data controller should', APEC says 'member economies should consider encouraging'. APEC allows appropriate safeguards to be limited by also 'take[ing] into account the potential harm to individuals'. Whereas OECD simply states that controllers 'should' notify significant security breaches, APEC limits itself to stating that member economies 'should consider encouraging or requiring' such notice [58].

APEC CBPRs: A failed 'accountability mechanism'

The *Secretariat Background Paper* [7] notes that the explanatory memorandum to the 2013 OECD Guidelines state that the APEC CBPRs is a model for the role an accountability scheme can play in 'giving binding effect to the Guidelines to enable transborder data flows.'

---

[5] CIPL 'OECD-CIPL Expert Consultation on Accountability: Background Discussion Paper', p.3. (*OECD Expert Consultation on Accountability, 6 May 2019, 'Room Document', unpublished).*

[6] ibid, p. 2.

Docksey describes APEC CBPRs as an 'accountability mechanism, certified by an APEC-recognised independent third party known as an Accountability Agent'.[7] This government-nominated Accountability Agent (AA) then certifies that individual companies (in the economy concerned) that apply to be certified, do comply with the APEC Framework principles, and related procedural requirements. The AA carries out dispute resolution and enforcement activities, and renews certifications annually. The AA is intended to self-fund its activities from fees.

Many criticisms can be made about the operation of APEC CBPRs[8] but need not be made here because the simple fact that needs to be stated is that this accountability mechanism is at this stage a near-complete failure. After being in operation for seven years, only two countries – the USA and Japan – participate fully, in that they have nominated an AA and that AA certifies companies. Even the participation of these two countries should be classified as a failure, since only 24 US companies[9] have been certified since 2013, and 3 Japanese companies[10] since 2015. It appears that companies cannot find a business case to justify the fees.

APEC economy	Approved to join APEC-CBPRs	Accountability Agent appointed	No. of Companies certified
USA	**2012**	**2013**	**24**
JAPAN	**2014**	**2015**	**3**
CANADA	2014	–	0
MEXICO	2014	–	0
KOREA	2016	–	0
SINGAPORE	2017	–	0
TAIWAN	2018	–	0
AUSTRALIA	2018	–	0
OTHER 11 IN APEC	–	–	0

Six other countries – including Mexico and Canada as long ago as 2014 – have taken preparatory steps to be involved, but have not appointed an AA, and consequently none of their companies have been certified. Could it be that there is no business in these economies that thinks there is a good business case for becoming an AA? No doubt many creative excuses are provided at APEC meetings in response to US questions concerning non-appointment of an AA.

Transparency of complaint resolution in APEC CBPRs: Missing in action

There are two aspects of the operation of APEC's CBPRs which go directly to the questions of whether either its Accountability Agents, or the companies they certify, really are 'accountable' in the sense of having any liability for failure to comply with CBPRs rules:[11]

[7] Docksey, op cit.

[8] See for example G. Greenleaf, 'APEC's Cross-Border Privacy Rules System: A House of Cards?' (2014) 128 *Privacy Laws & Business International Report*, 27-30 <https://ssrn.com/abstract=2468782 >.

[9] TrustAct *APEC CBPR Certified Companies* < https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list> as at 7 January 2019.

[10] See JIPDEC's APEC CBPRs Certified Companies list <https://english.jipdec.or.jp/protection_org/cbpr/list.html> (as at 7 January 2019).

[11] Extracts are from G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), p. 533.

> '10. An AA is required to investigate complaints made to it against a company it has certified, and to remove the certification of companies that fail to remedy breaches of the programme requirements within a reasonable time. The AA is required to refer a breach which has not been remedied in a reasonable time to an appropriate PEA 'so long as such failure to comply can be reasonably believed to be a violation of applicable law',[12] which leaves considerable discretion to the AA. An AA is not required to have the ability to impose financial penalties on companies in breach,[13] and there is no requirement to be able to award compensation to consumers. Therefore, the only additional remedy that the CBPR offers consumers is that a company might have its certification removed.'
>
> '11. AAs are required to 'release anonymised case notes ('on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes') and complaint statistics'.[14] This transparency, if made effective,[15] could be a strong point of APEC-CBPRs.'

The only place that this accountability can be demonstrated, particularly in the sense of the transparency that is part of the concept of accountability, is on the web pages of the USA's AA, TrustArc (formerly TRUSTe),[16] because it has at least certified 24 companies, and some for up to six years. Those web pages do include a form by which data subjects can lodge a complaint with the AA concerning a certified company, but they do not contain any information at all about any of the matters set out in 10 and 11 above. Even if the system is working without a single flaw, a statement to this effect should be made.

CBPRs is not a plausible basis for interoperability

The potential for 'interoperability' between CBPRs and other international instruments concerning data protection, is mentioned in Background Papers and the Guidelines themselves. However, CBPRs are too low a standard to suit this purpose, as can be inferred from the EU 's adequacy decision concerning Japan, and from the A29WP 'Referential' of 2014.

Japan's PPC (its DPA) had provided by delegated legislation that transfers of personal data by Japanese companies to overseas (currently, US) companies that had been certified under APEC CBPRs, would be considered to have adequate protection under Japanese law. The European Commission, in its final adequacy Decision concerning Japan, concluded that:[17]

> … outside the cases where the PPC has found that the third country in question ensures a level of protection equivalent to the one guaranteed by the APPI [Japanese law], the requirements set forth in Supplementary Rule (4) exclude the use of transfer instruments that do no[t] create a binding relationship between the Japanese data exporter and the third country's data importer of the data and that do not guarantee the required level of protection. This will be the case, for instance, of the APEC Cross Border Privacy Rules (CBPR) System, of which Japan is a participating economy, as in that system the protections do not result from an arrangement binding the exporter and the importer in the context of their bilateral relationship and are

---

[12] *APEC Accountability Agent Recognition Criteria* (APEC, undated), criterion 14.

[13] JOP determination of TRUSTe AA application, 2013.

[14] *APEC CBPR System – Policies, Rules and Guidelines* (APEC, undated), p.15; *APEC Accountability Agent Recognition Criteria* (APEC, undated), criteria 10(g) and 10(h).

[15] APEC's JOP initially agreed to allow TRUSTe to publish statistics on larger sets of data, not only APEC-related complaints, which would have 'buried' the APEC data. After criticisms from civil society organisations, they reversed this: APEC CBPRs JOP 'Recommendation Report on APEC Recognition of TRUSTe' (JOP, 18 June 2013), pgs. 15-16.

[16] TrustArc 'TRUSTe APEC CBPR and PRP Privacy Certifications' < https://www.trustarc.com/products/apec-certification/>

[17] EC para (79)

> clearly of a lower level than the one guaranteed by the combination of the APPI and the Supplementary Rules.' [footnotes in original omitted]

While the EC does not explicitly say that the content of APEC CBPRs protections do not provide a level of protection which cannot be considered to be 'adequate' under the GDPR, that is clearly the implication. The reference to the 'lower level' CBPRs standards in the above quotation is footnoted as follows: 'For example, no definition and specific protections for sensitive data, no obligation of limited data retention' (FN 50). The suggestion that APEC CBPRs might be 'interoperable' with the EU GDPR seems therefore to be on very shaky foundations.

The A29WP 2014 'referential' on CBPRs[18] compared with EU BCRs (Binding Corporate Rules) under the (then) Directive does not provide, on my interpretation,[19] any basis for optimism that any form of 'interoperability' between the two would ever be found. The Referential also pre-dates the CJEU's *Schrems* decision in 2015, which could raise the standards required of BCRs.

CIPL argues[20] that:

> '…BCR, CBPR, PRP, Privacy Shield and future GDPR certifications or codes of conduct, enable responsible cross-border data transfers. They are (or can be) designed to meet an agreed privacy standard of multiple jurisdictions and to serve as a recognised cross-border transfer mechanism in jurisdictions that impose data transfer restrictions in their privacy laws. They can and should also be made interoperable with each other.'

This argument rests on the false assumption that these instruments implement the same data protection standards. They do not, as argued above, because APEC CPBR implements a manifestly lower standard than the GDPR. It can also be argued that it is a lower standard than Convention 108+ (or Convention 108), or in Africa the standards found in the ECOWAS Supplementary Act or the African Union Convention dealing with data protection. The CIPL conclusions concerning cross-border transfer mechanisms, and concerning interoperability therefore do not follow and should be rejected.

This argument also has implications for the OECD Guidelines, because they also implement what are essentially the same low standards as the APEC Framework and APEC CBPRs.

---

[18] Article 29 Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents, 6 March 2014. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf>.

[19] G. Greenleaf, 'APEC's Cross-Border Privacy Rules System: A House of Cards?' (2014) 128 *Privacy Laws & Business International Report*, 27-30 <https://ssrn.com/abstract=2468782 >. My conclusions concerning the differences revealed by the Referential are: 'For each of 27 separate 'essential principles and requirements' of BCRs and/or CBPR, the referential lists both a 'common block' of elements which are 'common or similar' to the two, and 'additional blocks' of differences between the two or additional elements specific to each. The starting point for an assessment is that 26 of the 27 'essential principles and requirements' have 'additional elements' listed. In number 27 there is complete unanimity that an organisation's privacy rules must specify their effective date. In almost all of the other 26, the text of the additional elements is longer than the 'common block', in most cases far longer. In principles 9 and 11 they are roughly of equal length. In most cases it is the EU's additional requirements that are longer. In some cases there is no 'common block' at all, such as the very significant number 4, 'Requirements for data subjects and third party beneficiary rights'. While it is obviously necessary to read the 62 pages of the referential to gain a proper impression of how significant these differences are, it is beyond doubt that there are such wide differences that a lengthy period of study is required even to understand them, let alone build bridges to overcome them.'

[20] CIPL op cit p. 7.

4. Addressing accountability gaps in the OECD Privacy Guidelines

The conclusions which I suggest can be drawn from this discussion are that the 2013 Guidelines should be further amended as follows:

1. The Guidelines should clarify that the demonstration of a privacy management programme (PMP) is an additional and separate obligation, and that failure to comply with it will involve consequences (liability)

2. The Guidelines should clarify that accountability, in the context of the Guidelines, is always an obligation owed to a specified party or parties, namely to data subjects and/or to the relevant privacy enforcement authority (PEA), depending on the particular right or obligation to which accountability applies.

3. The Guidelines should clarify that accountability, in the context of the Guidelines, always involves legal consequences for failure to comply (liability) with any aspect of accountability. However, accountability may also apply to non-enforceable means of implementation in addition (for example, some codes of conduct, and standards).

4. The reference in the Guidelines to APEC CBPRs as a model of accountability implementation should be withdrawn, at least until there is evidence of credible-take up and implementation.

5. The Guidelines should not suggest that APEC CBPRs is a possible basis for a form of 'interoperability' with other regional or global data privacy instruments (other than with the current OECD Guidelines).