

University of New South Wales
University of New South Wales Faculty of Law Research Series
2012

Year 2012

Paper 57

Obama's Privacy Framework: An offer to be
left on the table?

Graham Greenleaf*

Nigel Waters†

*University of New South Wales

†University of New South Wales

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps12/57>

Copyright ©2012 by the authors.

Obama's Privacy Framework: An offer to be left on the table?

Graham Greenleaf and Nigel Waters

Abstract

The Obama Administration is offering the rest of the world a deal: 'global interoperability', comprising 'mutual recognition and enforcement cooperation'. Perhaps we should read the small print. The 'Framework' initiative (*Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, The White House, Washington, February 2012), launched in early 2012, represents a new level of serious consideration of privacy protection by a US Administration. While it is difficult to assess how much of it it is likely to be achieved in the face of both political gridlock and constitutional uncertainties, it is clearly in the interest of Americans that their government is attempting to take these steps to improve domestic privacy protections. But does this initiative offer sufficient of value to the rest of the world, for the price of 'interoperability'?

This article looks at the proposed Framework from the following explicitly 'non-US' perspectives:

- (i) Does the Framework's 'Consumer Bill of Rights' meet international standards?
- (ii) Is the proposed method of achieving it realistic or futile?
- (iii) Is the US demand for 'interoperability and mutual recognition' reasonable?
- (iv) Is the USA ever likely to protect privacy to international standards?

The article concludes that the rest of the world has to accept that there are some aspects of US domestic law on data privacy which are unlikely to change, but

that does not constitute a reason for reducing international privacy standards in fundamental ways in order to accommodate the weaknesses of American privacy protection. The US approach does not deserve an undue amount of respect simply because of its economic and political power, and the Framework proposals do not at this stage change that. A better approach is to support those seeking reform in the USA by deferring 'interoperability' until US standards are in practice somewhere closer to those being adopted by most other countries. At some point it could become a rational decision that to have the USA implement and enforce significantly better CPBR would be a deal worth making, for the benefits of 'interoperability' on the basis of a minimum global standard. But at the moment that is not the right, best or only choice.

Obama's Privacy Framework: An offer to be left on the table?

Graham Greenleaf & Nigel Waters*

Privacy Laws & Business International Report, Issue 119: 6-9, October 2012

The Obama Administration is offering the rest of the world a deal: 'global interoperability', comprising 'mutual recognition and enforcement cooperation'. Perhaps we should read the small print. The 'Framework' initiative¹ launched in early 2012 represents a new level of serious consideration of privacy protection by a US Administration. While it is difficult to assess how much of it it is likely to be achieved in the face of both political gridlock and constitutional uncertainties, it is clearly in the interest of Americans that their government is attempting to take these steps to improve domestic privacy protections. But does this initiative offer sufficient of value to the rest of the world, for the price of 'interoperability'?

This article looks at the proposed Framework from the following explicitly 'non-US' perspectives:

- (i) Does the Framework's 'Consumer Bill of Rights' meet international standards?
- (ii) Is the proposed method of achieving it realistic or futile?
- (iii) Is the US demand for 'interoperability and mutual recognition' reasonable?
- (iv) Is the USA ever likely to protect privacy to international standards?

Would the 'Consumer Bill of Rights' meet international standards?

The Framework's 'Consumer Privacy Bill of Rights' (CPBR) comprises seven principles, marked in italics below, as described in Framework's summary. We will initially ask whether each one meets the standard of the OECD Privacy Guidelines of 1981.² OECD is the lowest standard on which any international accommodation could reasonably be based, and one to which the USA is already ostensibly a party.

- (i) *Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.* The detailed CBPR principle do not mention 'consent' until the last sentence, leaving it quite ambiguous whether positive consent is ever required, or can always be supplanted by the 'choice' provided by the opportunity to opt-out. The OECD Guidelines do not elevate 'choice' to a separate principle, though they make 'consent' important to collection, use and disclosure. While giving consumers choice is *prima facie* valuable, it is unclear whether the CPBR principles allow choice to override other principles (eg security, or access), which is dangerous, and is not OECD-consistent. Where choice is reasonable, within a particular principle, the default condition within which choice operates (particularly 'opt-in' or 'opt-out' concerning secondary uses) is also crucial. The CPBR says nothing on this, and (in an example) wrongly asserts that, in SNS, 'the use of personal data begins with individuals' decisions to choose privacy settings', whereas in fact it begins with the

* Professor of Law & Information Systems, University of New South Wales, and JSPS Visiting Fellow, Centre for Business Information Ethics, Meiji University, Tokyo; and Principal Consultant, Pacific Privacy, respectively.

¹ *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, The White House, Washington, February 2012

² OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Part 2. Basic principles of national application,

default settings determined by the SNS operator. Many business models are too difficult to explain and to offer meaningful choices. Choice is not a panacea.

- (ii) *Transparency: Consumers have a right to easily understandable and accessible information about privacy and security practices.* This is similar to the OECD's Openness principle. Both are deficient in not requiring consumers to be given notice of the purpose of collection, in contrast with the EU privacy Directive requirement that the data subject must be given information including the purpose of collection of the data 'except where he already has it'. Even the APEC privacy principles require notice to be given of the purpose of collection. This deficiency allows other CPBR principles to be more vague and elusive.
- (iii) *Respect for Context: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.* Without any explicit requirement of notice of the purpose of collection, the CPBR allowance of changes of use, or external disclosures, wherever they are 'consistent' with the context of collection, and without requiring consent (only 'appropriate levels of transparency and individual choice'), becomes elusive indeed. Interpretations favoured by commercial interests are likely to prevail in any unbalanced multi-stakeholder consultation. The CPBR demonstrates this risk by arguing that it is OK for SNS companies to reveal some personal information about members without consent, to 'help them form new connections' and OK for companies to use consumer data to create new services wherever customers would expect such new services. The OECD's Purpose Specification and Use Limitation principles, which together make up the core condition of 'finality' in data processing, are not captured by these CPBR principles, although they claim to be based on them. The stronger requirements of the EU Directive, requiring collection for specific and explicit purposes, are even more divergent, so these issues remain major points of difference between the USA and Europe.
- (iv) *Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain – 'only so much as they need to accomplish purposes specified under the Respect for Context principle'* says the detailed principle. This is stronger than the OECD Collection principle which only requires that collection should be 'limited'. On its face, it is closer to European principles requiring 'minimality' in collection, but the problem (as discussed above), is that CPBR does not require purposes to be 'specified' in any meaningful way. Both CPBR and OECD need to put a greater onus on organisations to justify collection and processing in relation to stated purposes. Otherwise, retrospective justifications will be too readily accommodated.
- (v) *Security: Consumers have a right to secure and responsible handling of personal data.* This matches the OECD's Security Safeguards principle, including a statement of the risks against which data must be secured.
- (vi) *Access and Accuracy: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.* The inclusion of a 'likelihood of harm' test is not found in the OECD 'Individual Participation' principle or in almost any other privacy laws. It diminishes the effect of 'individual control' element as a fundamental right, irrespective of harm.
- (vii) *Accountability: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the [CPBR].* This more precisely states the OECD's Accountability Principle, but the detailed principle grafts on

an APEC-like addition, that companies disclosing personal data (whether within the US or exporting it overseas) should 'at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these [CPBR] principles'. It says nothing about the exporter of data retaining any liability for breaches by the importer. Although a third parties may enforce contractual obligations made for their benefit under US law, it will be of little comfort to consumers that they can sue an overseas data importer for possible misuse occurring overseas. This form of data export limitation is not accepted as an adequate substitute for a 'border control' approach by most countries with data privacy laws.

In a few respects, the CPBR goes beyond the OECD requirements, including significant steps toward deletion principles such as Individual Control principle's 'right to withdraw consent', and the Transparency principle's notice of policies on deletion and de-identification.

These seven CPBR principles do, on their face, include elements of each of the OECD's seven 'Principles of National Application', but almost all with weaknesses. The key deficiency is that 'Respect for Context' falls short of the 'finality' principles, the combination of Purpose Specification, Use Limitation and Collection Limitation. The CPBR does not therefore adequately meet the basic international OECD standard.

However, even if CPBR was considered to equate to OECD, why should the rest of the world settle for a bargain based largely on a model from the early 1980s? Since then, most of the more than 90 countries that have enacted data privacy laws³ have moved beyond the OECD principles toward what can be called the 'European principles', embodied in both the EU privacy Directive and the Council of Europe Convention (with its 2001 Additional Protocol)⁴. These add significantly stronger principles, particularly the 'adequacy'/border control limitations on data exports, 'minimality' in collection, and deletion, plus specific enforceability requirements such as an independent data protection authority (DPA) and recourse to the courts.

We must therefore question whether, even if the Framework's seven CPBR principles were credibly implemented, this would in itself justify the rest of the world going 'back to the 1980s' to a lower standard for global data privacy 'interoperability' than has been, in practice, already accepted by a most countries with data privacy laws.

It could be a rational decision that to have the USA implement and enforce a defective version of the OECD Guidelines (plus a little more) would be a deal worth making, but it is not necessarily the right, best or only choice. It would be a better deal if the USA was offering a 'Respect for Context' principle that implemented genuine 'finality', an unequivocal right of access, plus more elements that go beyond the OECD basics including at least real enforceable 'accountability' by consumers in relation to data exports. The present CPBR is good on the less important principles, but defective on all the key elements.

Is the proposed implementation of the Framework futile?

Whatever view one takes of the adequacy of the Framework's CPBR principles, they are merely a set of aspirations as yet. They should not have credibility until it is clear that the USA can and will deliver them. There are reasons to be sceptical that this will ever happen. There is always hope, and privacy advocates in the USA have little choice but to work for that hope to be realised. But the rest of the world should keep its pen in its pocket until the hope of credible enforcement is fulfilled.

³ Greenleaf, G (2012) 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' *International Data Privacy Law*, Vol. 2, Issue 2, 2012, also available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299>

⁴ *ibid*

President Obama says his Administration will 'work with Congress to put [the CPBR] into law', but the Framework's approach places too much faith in a 'multi-stakeholder' collaborative process designed to achieve consensus, and a large component of self-regulation, which can only sometimes be supported by FTC enforcement (and then become co-regulation). But commercial interests in exploiting personal information are too strong to be voluntarily made amenable to the necessary levels of participation and control by individual consumers. The Framework seems designed to accommodate most new business models, rather than subjecting them to a test of consistency with privacy principles. Some business models, particularly in the online world, are incompatible with privacy rights and should not be permitted. The entire approach will be very slow and uncertain, giving businesses another 3-4 years to 'lock in' unacceptable business models and create consumer dependency. There is a strong risk of repeating previous regulatory failures. US commentators (including Swire and the World Privacy Forum⁵) have demonstrated that industry attention to making self-regulation work only waxes when threats of regulation appear, and wanes as soon as the threat diminishes.

Multi-stakeholder consultation to develop codes favours well resourced business interests over poorly resourced civil society, with no realistic prospect of consensus on some key issues. Codes of practice/conduct have been tried as privacy protection (and as consumer protection generally) in many jurisdictions, without much success in providing acceptable levels of practical protection.

Reliance on FTC enforcement is also inadequate, for many reasons. It can only work against businesses that adopt codes, with no redress against 'cowboys'. The FTC has limited jurisdiction, with major sectoral gaps, and even then the actions available to it may not allow enforcement of all principles/elements in a comprehensive privacy regime. Such actions are also ineffective against third party data controllers with no direct interaction with the consumer, unless they can be persuaded to make representation to consumers concerning their personal information practices. FTC action is triggered primarily by complaints, but pro-active 'own-motion' investigations are also needed. It has failed to enforce a number of its own orders.

Even if this 'multi-stakeholder' approach is the best that can be delivered in the current US political and legal context, and so US parties have to make the best they can of it, why should the rest of the world assume that such a peat bog of uncertainty will deliver useful results? Countries other than the USA do not have this severe disability because they can and do legislate. The USA's 'preferred' approach should not be given undue weight. 'Wait and see' is the only prudent response.

'Interoperability & Mutual Recognition' – Mistaking a result for a condition

Where two parties (say, Universities in different countries) decide after their own assessment that the standards applied by the other are of approximately the same quality standard as their own, they may extend to each other 'mutual recognition' of standards, and consequent 'interoperability'. However, if 'interoperability and mutual recognition' is presented simply as a demand, it is just intimidation, the attempt by the stronger party to impose its standards on the weaker party. Is the USA's desire for 'interoperability and mutual recognition' a demand that overseas regulators should accept the US model and allow data transfers to US companies without further assessment of individual circumstances?

The Framework suggests the APEC Cross Border Privacy Rules (CBPR) as a basis for mutual recognition and interoperability. But even if we accept APEC's own terms, this 'interoperability' will only be forthcoming if other APEC members agree that the US principles and enforcement package meets the criteria for participation, which requires two more milestones to be met (see article by Waters in this issue). It may also require other APEC members with tougher data export

⁵ See testimony by Peter Swire to Congress in this issue, and references to WPF studies cited therein.

restrictions in their privacy laws interpret (or change) those laws to recognise APEC CBPR as 'adequate' without further assessment (contrary to promises not to weaken existing laws). There are therefore reasons why APEC CBPR may be of a low standard, if it ever eventuates.

How severe are the limits on the USA's ability to protect privacy?

The USA has many privacy laws and some effective enforcement, but no comprehensive privacy law for its private sector. There is an arguable case that, even if all of the USA's existing sectoral laws (including FTC protections and privacy torts) were consolidated into one Act, and even if that Act was extended to the whole of the private sector, the standards it would embody would currently fall short of both the OECD Guidelines and 'European standards' in fundamental respects. The lack of general application of the 'finality' principles makes it unlikely that the USA has complied with the OECD guidelines in relation to its private sector,⁶ although no full study has been done to establish this.

The current legislative gridlock in relation to laws imposing greater regulation on the private sector makes it unlikely this will change soon, but it is also arguable that there are constitutional reasons (based primarily on the First Amendment) why US data privacy laws are never likely to approximate those common in Europe and elsewhere. There is considerable disagreement between US scholars on the extent, if any, of constitutional restrictions on disclosure, use and collection of personal information by the private sector (and perhaps by the States).⁷ The US Supreme Court's recent decision in *Sorrell v. IMS Health Inc.*, 131 S.Ct. 2653, 2672 (2011), which found that a state law that prohibited the sale of information on doctors' prescribing habits to marketers for drug companies violated the First Amendment resulted in arguments that the principles of *Sorrell* 'strongly suggest that any such legislation [as the Bills currently before Congress] would run afoul of the First Amendment'.⁸ However, it has been vigorously argued that more narrow readings of the decision are correct and that the majority of these bills would pass constitutional scrutiny.⁹ The extent of constitutional limitations on the scope of data privacy laws in the USA is clearly not yet settled (and beyond the expertise of the authors), but they may be significant.

It is therefore important for any non-US parties considering the interoperability 'offer', to recognise both that there may be existing fundamental differences between US and other laws, and that it is possible that US privacy standards have inherent limitations of uncertain scope which are likely to make these fundamental differences continue. Given that 'known unknown', any accommodation between US and European standards needs to be based on proven achievements, not on objectives that may not be capable of being realised.

What attitude should the world take to the USA's privacy limitations?

These limitations do not mean that the USA lacks privacy standards or privacy innovations. R E Smith gives a succinct but lengthy catalog of where US laws have pioneered particular privacy protections, often with laws that are stronger than elsewhere.¹⁰ The role of the Federal Trade Commission (FTC) in enforcing some voluntary privacy commitments by companies also gives 'self regulation' in the USA a different meaning from elsewhere (as Peter Swire notes in this issue), more akin to co-regulation. The USA is a country with a unique approach to data privacy which has

⁶ See Greenleaf (2012) op cit for the argument in support of this proposition.

⁷ Greenleaf (2012) gives a summary of this argument, and references.

⁸ Julin, T 'Sorrell v. IMS Health May Doom Federal Do Not Track Acts' *BNA Privacy and Security Law Report*, 10 PVLR 1262, 09/05/2011

⁹ Cole, A 'Internet advertising after Sorrell v IMS Health: A discussion on data privacy & the First Amendment', *30 Cardozo Arts & Ent. L.J.* 283 (2012), available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2079079>

¹⁰ Smith R E 'Letter to the Editor' *Privacy Laws & Business International Report*, Issue 113, October 2011

resulted in an inconsistent patchwork of laws, usually with some key standards weaker than is common in the rest of the world (particularly limits on collection, secondary use, disclosure and data exports). The USA's approach has not until now provided an alternative paradigm for data privacy, and as a result it is increasingly isolated in taking that approach.¹¹

These differences between the USA and the rest of the world are amplified by the core role the USA plays as the host or provider of numerous Internet-based personal information services with global reach. The attempt to make US-based services accommodate the data privacy approaches of most other countries will continue to be one of the defining features of global privacy developments for years to come. Conversely, attempts by US companies and the US government to use their combined economic and political influence to limit development of data privacy laws in other countries will continue to be important, but may now be 'swimming against the tide'.

The rest of the world has to accept that there are some aspects of US domestic law on data privacy which are unlikely to change, but that does not constitute a reason for reducing international privacy standards in fundamental ways in order to accommodate the weaknesses of American privacy protection. The US approach does not deserve an undue amount of respect simply because of its economic and political power, and the Framework proposals do not at this stage change that. A better approach is to support those seeking reform in the USA by deferring 'interoperability' until US standards are in practice somewhere closer to those being adopted by most other countries.

At some point it could become a rational decision that to have the USA implement and enforce significantly better CPBR would be a deal worth making, for the benefits of 'interoperability' on the basis of a minimum global standard. But at the moment that is not the right, best or only choice.



¹¹ See Greenleaf, (2012)