Australian Privacy Foundation

Consumer Data Privacy in a Networked World[1]

Australian Privacy Foundation Submission on US Administration White Paper and associated Consumer Privacy Bill of Rights

April 2012

The Australian Privacy Foundation (www.privacy.org.au], through its International Committee[2], welcomes the initiative taken by the US Administration in moving to a new level of serious consideration of privacy protection. The proposed regime nevertheless still falls well short of international best practice. We make the following submission, which concludes by recommending that the Administration abandons its current approach in favour of enactment of a comprehensive private sector privacy law to the maximum extent constitutionally possible. If the Administration nonetheless proceeds with its favoured approach, it should address the weaknesses outlined in this submission.

- The Administration's approach places too much faith in a collaborative process designed to achieve consensus. Commercial interests in exploiting personal information are simply too strong to be amenable to levels of participation and control by individual consumers that meet community expectations. We submit that the proposed framework seems designed to accommodate most new business models, rather than subjecting them to a test of consistency with fundamental privacy principles. It should be recognised from the outset that some business models, particularly in the online world, are simply incompatible with privacy rights, and would not be permitted by an effective privacy regulatory framework.

- The entire approach is too slow, and too uncertain, to deal with pressing privacy protection needs. It will simply give businesses another 3-4 years to 'lock in' unacceptable business models, creating consumer dependency which will prevent individuals from making the sort of choices in respect of use of their personal information that they deserve to enjoy.

[1] See http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights and http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[2] The APF International Committee is made up of internationally recognised privacy experts Chris Connolly, Roger Clarke, Graham Greenleaf, Dan Svantesson, David Vaile and Nigel Waters – see http://www.privacy.org.au/About/Contacts.html#Officers.

- Giving business interests another chance to come up with yet another essentially self-regulatory response, even if this is backed up with stronger enforcement, repeats regulatory failures to date, and is an insufficient response to an urgent problem.

- Reliance on Codes is a flawed approach:
    - Multistakeholder consultation favours well resourced business interests over poorly resourced civil society NGOs
    - There is no realistic prospect of consensus on some key issues
    - We note that Codes of practice/conduct have been tried as a means of privacy protection (as well as consumer protection more generally) in many jurisdictions, almost always without success in providing acceptable levels of practical 'on the ground' protection.
    - Reliance on FTC enforcement inadequate, for several reasons:
      - it can only work against businesses that adopt codes - no redress against 'cowboys'
      - the FTC has limited jurisdiction - major sectoral gaps
      - there is great potential for confusion if a business is subject to multiple codes/laws
      - action for 'unfair or deceptive' acts or practices, or inadequate security may not allow enforcement of all principles/elements in a comprehensive privacy regime that implements the 1980 OECD Guidelines
      - action for 'unfair or deceptive' acts or practices is ineffective against third party data controllers with no direct interaction with the consumer
      - FTC action is triggered primarily by complaints – this is inadequate for privacy issues – effective enforcement requires a greater capacity, and resources, for pro-active 'own-motion investigations
      - we understand that the FTC has failed to enforce a number of its own orders

- The Consumer Privacy Bill of Rights is a welcome and mostly positive initiative. However, the wording of its principles allows much room for argument about meaning and compliance standards.

- In particular, 'Respect for Context' appears to favour 'consumer expectation' but will be used by businesses to argue for complex business models – the outcome will depend on interpretation of 'consistent with the context', and interpretations favoured by commercial interests are likely to prevail in any unbalanced multistakeholder consultation.

- The scope of application needs to be clarified. It is essential that 'personal data' is defined clearly to include any data which either alone, or in combination with other data that can be obtained by an organisation, allows either the identification of individuals or actions in relation to individuals targeted on the basis of individual data. Existing narrower definitions of personal data in most privacy instruments and laws allow too many technologies and business models to avoid the application of privacy principles. It is important that the new Bill of Rights addresses this issue.

- While there appears to be some recognition of the weakness of reliance on 'notice and consent' we submit that the Bill of Rights still places too much reliance on these as a basis for processing personal information. The reality is that many business models are just too difficult to explain and to offer meaningful choices. Effective privacy protection in our view requires a default position of 'opt-in' rather than opt-out' for secondary uses, with a very narrow definition of 'primary purpose'.

- There needs to be a greater onus on organisations to justify collection and processing of personal data on the basis of relevance and proportionality – without this, self serving

justifications, based on however organisations choose to package their commercial offerings, will be too readily accommodated.

- The 'Individual Control' principle must apply not only to personal data collected from the data subject but also to personal data acquired from third parties or generated by an organisation from transactions – in other words it must apply to all personal data, broadly defined.

- The access and accuracy element is heavily qualified, and falls short of the default presumption of access and correction in most privacy laws. Individuals should also have the right to have the logic of any processing explained to them.

- The inclusion of a 'likelihood of harm' test in the access and accuracy element in relation to choices is dangerous – it diminishes effect of 'individual control' element as a fundamental right, irrespective of harm.

- There should be an express requirement to delete or irrevocably de-identify personal data once it is no longer required for the original primary purpose or any legally authorised secondary purposes.

- In respect of Interoperability & Mutual Recognition, it is difficult to argue with the general wording and objective - but history suggests that this is a 'coded' cover for requiring overseas regulators to accept US model and allow data transfers without independent assessment of whether there really are equivalent standards and enforcement in place.

- We note the specific reference to the APEC Cross Border Privacy Rules (CBPR). These will only 'work' as the paper suggests is intended if other APEC members agree that the US principles/enforcement package (i.e. CBPR program standards assessed by an accountability agent (e.g. TRUSTe) and enforced by a regulator such as the FTC) meets the criteria for participation. Whether this agreement is forthcoming remains to be seen, and could in any case only be partial - for businesses within FTC jurisdiction. It will also only work as intended if other APEC members with tougher data export restrictions in their privacy laws interpret (or change) those laws to recognise APEC CPBR as 'adequate' without further assessment - participants in the APEC privacy work have consistently offered re-assurance that there is no intention of weakening or circumventing domestic laws, yet this is the only way that the CBPR system could work fully as seems to be intended.

- We submit that the Administration should abandon its flawed approach to private sector privacy protection based on a slow, piecemeal co-regulatory approach and instead join the trend in most other jurisdictions towards a comprehensive statutory approach with binding privacy rules applying to all commercial sectors, and a well resourced independent data protection supervisory authority with strong enforcement powers.

- If the Administration proceeds with the approach outlined in the White Paper, it should acknowledge and address the many potential weaknesses and flaws outlined in this submission.

For further contact on this submission - Nigel Waters, +61-2-4981-082, board5@privacy.org.au