Senate Committee Follow Up Questions – Privacy Bill Submission

1. Your submission claims that the use of anonymity and pseudonymity under APP 2 will prevent organisations from maintaining accurate and up-to-date records of personal information. In your view, are there any situations in which anonymity and pseudonymity should be permitted? What is the appropriate balance between allowing anonymity and pseudonymity while maintaining accurate information?

Our primary concern with APP 2 is that the apparent drafting error in APP2.2(b) and the Explanatory Memorandum (EM) is corrected. APP2.2(b) and the EM should reflect both anonymity and pseudonymity, as indicated in APP2.1, not just anonymity.

Our submission also requests that the EM be amended to clarify that whether it will be impracticable to enable anonymous or pseudonymous use will depend on the circumstances and context.

It would also be helpful to clarify in the EM that it will be impracticable to do so:

a) for opt-in services that rely on a real name culture as an essential part of their service, for example, to help people find and connect with each other and to promote user safety and security. An example of this is Facebook. In their recent audit of Facebook the Irish Data Protection Commissioner confirmed that requiring real names and identities was necessary for child protection and related safety reasons; and,

b) for organisations operating ecommerce websites where there is a need for users to authenticate their identity through the use of credit cards.

There are other circumstances where anonymous or pseudonymous interaction will be appropriate. One example is use of the Google search engine where a user chooses not to be signed into their Google account.

It is not appropriate to exhaustively set out in advance the circumstances in which anonymity or pseudonymity is practicable and when it is not. This must remain flexible and be assessed on a case by case basis.

2. Your submission argues that it is not possible to include an opt-out statement in each direct marketing communication to an individual, as required under APP 7.3, where communication is through emerging technologies and social media. How do you think direct marketing through social media (e.g. Twitter) and online advertising should be regulated? What opt-out options would be more appropriate in these settings?

We believe that there needs to be greater clarity around what activity constitutes direct marketing and what activity does not. In the process of seeking clarity around what constitutes direct marketing, it appears that customised marketing – which is a key driver of Australia's digital economy, drives economic efficiencies for advertisers, and leads to increased consumer satisfaction – is being misunderstood as direct marketing. Industry undertakes a range of educational initiatives around how online advertising works and offers consumers a range of tools to control their online experience, including with respect to advertising. We have provided some specific wording to assist the Committee to rectify this misunderstanding.

Our concerns with APP7 are:

a) there should be a definition of 'direct marketing'. We provide a potential definition in our written submission.

b) there appears to be a drafting error in the opt-out requirement. The opt-out should be from 'direct marketing that relies on personal information', not from direct marketing altogether.

3. Can you explain your concerns regarding the potential application of APP 8 to entities operating from overseas who collect personal information from individuals within Australia? What clarifications are needed in relation to this issue?

Our concerns around APP8 are two-fold:

- The imposition of strict liability on companies who have taken all reasonable steps to ensure that overseas recipients comply with the APPs; and
- That APP8.2 does not reflect the ability of an individual to seek recourse through the Australian Privacy Commissioner via cross-border enforcement arrangements (current and future) such as the APEC Cross Border Privacy Enforcement Arrangement (CBPEA).

With respect to the first concern, we request that a defence is introduced into the Bill in circumstances where an entity can demonstrate that they took all reasonable steps to ensure compliance with the APPs during a cross border transfer. Failing that, we ask that guidelines be issued to the Commissioner around what matters ought to be considered in assessing the consequences of a breach under these circumstances.

On the second point, we ask that APP8.2(a)(ii) include an explicit reference to the ability for individuals to take action through the CBPEA by contacting their local privacy authority who can then pursue a cross border data issue with their counterpart in the relevant jurisdiction. In addition, we would welcome reference within this sub-section of APP8.2 to any additional recourse available to consumers contained within the APEC Privacy Pathfinder and any other arrangements entered into between privacy regulators.

4. Your submission argues that the Bill does not adequately allow for the requirements of foreign laws in relation to privacy protections. Can you explain how the bill could be amended to make it more consistent with overseas legislative regimes?

We welcome efforts to ensure consistency amongst privacy regulatory frameworks around the world. On the role of foreign laws, we respectfully ask that sections 6A(4), 6B(4) and 13D are amended to make clear in the Explanatory Memorandum that the term "applicable law of a foreign country" is (still) intended to cover the requirements of court orders, directions of regulatory agencies and other legally enforceable instruments made pursuant to an applicable law of a foreign country, as well as any direct application of that foreign law.