



Our reference: D2016/008675

Senator the Hon Ian Macdonald
Chair
Senate Legal and Constitutional Affairs Legislation Committee
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Senator

Submission on the Privacy Amendment (Re-identification Offence) Bill 2016

As the Australian Information Commissioner and Australian Privacy Commissioner, I welcome the opportunity to provide this submission to the Senate Legal and Constitutional Affairs Legislation Committee (the committee) in relation to its inquiry into the *Privacy Amendment (Re-identification Offence) Bill 2016* (the Bill).

At the outset, I would like to state that I am very supportive of the Australian Government's open data and innovation agendas. I recognise that increasing the availability of valuable government-held data may, in many cases, yield significant public benefits. However, I am also mindful that an appropriate balance must be struck between the interests of entities in having greater access to government-held data, and the privacy of individuals. This is particularly so where government-held data is collected on a compulsory basis (for example, where information is collected to enable provision of a government payment or service).

My Office has assisted numerous Australian Government agencies navigate the line between open data and privacy protection, including through the provision of advice and guidance. In this regard, we are currently updating our de-identification guidance materials,¹ and expect to release an updated de-identification resource for consultation in early 2017.

In this submission, I would like to raise some matters for the committee's consideration. By way of an overarching comment, I recognise that the Bill has the potential to be a privacy-enhancing tool by providing a deterrent against the intentional re-identification of certain datasets. However, for the reasons set out below, I believe that the introduction of new criminal offences and civil penalties, in and of itself, is unlikely to eliminate the privacy risks associated with the publication of de-identified datasets. Rather, additional measures will be

¹ See, eg, the OAIC's *Privacy business resource 4: De-identification of data and information* and the *Information policy agency resource 1: De-identification of data and information*, available at www.oaic.gov.au.

required for the policy objective of the Bill to be supported. In particular, under Australian Privacy Principle 1.2, agencies need to implement practices, procedures and systems to ensure that they comply with the *Privacy Act 1988* (Cth) (Privacy Act). That includes taking reasonable steps to ensure personal information is not disclosed through open publication.

The publication of de-identified information

The open publication of de-identified datasets may always present some level of risk. Effective de-identification requires a careful consideration of all relevant contextual factors, to help ensure that the risk of re-identification, as well as other threats to privacy, are minimised. This may include considering whether the risk of re-identification is sufficiently low to publish openly, or whether other safeguards should be applied, such as making the data available only to trusted users with contractual or technological safeguards in place. I therefore strongly encourage agencies to ensure that they take a wholistic and proactive approach to privacy throughout the information life-cycle, and in particular when determining suitable de-identification techniques and methods for releasing government datasets.

Strengthening privacy capability across the APS

As I have recently stated in other fora, I believe that the existing privacy capability of APS agencies to manage privacy risks may need to be strengthened. Agencies must have the capability to manage the personal information that they hold in accordance with the Privacy Act, and in accordance with the broader community's contemporary expectations. This is particularly relevant where Australian Government agencies may be considering whether and how to release valuable datasets which contain, or are derived from, personal information.

One way to enhance privacy capability across the APS, and in turn to support Australian Government agencies move towards best de-identification practice, is through the development of an APS-wide Privacy Code. In my capacity as Commissioner, I have the power under Part IIIB of the Privacy Act to approve or develop (in certain circumstances) a Privacy Code. A Privacy Code sets out how one or more of the APPs are to be applied, and/or can impose requirements additional to those contained in the APPs, in relation to specific activities, industries or professions.

A Code would be used to make explicit my expectations of agencies in relation to their obligations regarding a number of matters, creating additional clarity and accountability. In addition, a Code would enable agencies to move beyond a compliance approach and aim for best practice.

For example, a Code could require all Australian Government agencies to:

- have a privacy management plan
- appoint dedicated privacy contact officers to assist with day-to-day privacy matters
- appoint senior government officials as 'Privacy Champions' to provide cultural leadership and promote the value of personal information

- undertake written Privacy Impact Assessments (PIAs) where relevant
- keep a register of all PIAs conducted (and make this available to the Australian Privacy Commissioner on request), and
- take steps to enhance internal privacy capability, including by undertaking any necessary training, and conducting regular internal audits of personal information-handling practices.

General comments on the scope of the Bill

The Bill proposes to amend the Privacy Act to introduce new criminal offences and civil penalties for the intentional re-identification of government datasets that have been published on a de-identified basis, and other related acts.²

I note that as currently drafted, it is not clear how an Australian Government agency will establish that information 'was published on the basis that it was de-identified personal information'.³ As this is the central matter that will need to be established before an entity can be prosecuted, I recommend that the Committee consider how this issue could be addressed either through an amendment to the Bill, or in the implementation of the Bill. One way this could be done is through the development of a central register (for example, on data.gov.au) which would contain a list of datasets that have been published by agencies on a de-identified basis.

I understand that the entities subject to the Bill include all Australian Government agencies⁴ and all private sector organisations (including small businesses). In addition, individuals, including those acting in a private capacity, will be covered. The Bill therefore has a wider scope than the Privacy Act, which generally does not apply to small businesses or individuals acting in a private or non-business capacity.⁵

However, I otherwise understand that the majority of acts, practices, and/or organisations which are currently exempt from the application of the Privacy Act will also be exempt from the scope of the Bill. Acts or practices currently exempt from the Privacy Act include acts done by media organisations in the course of journalism; political acts and practices; and, as most Commonwealth legislation (including the Privacy Act) does not bind the States and Territories, the activities of state and territory bodies (including their employees) are also exempt. I note that the majority of universities in Australia are State and Territory bodies.

The scope of the Bill is therefore not comprehensive. Further, as I have said previously, privacy is now an international matter. Information flows have become more complex, traversing national borders and established regulatory jurisdictions. Where de-identified information is publically released, agencies should therefore be mindful that entities outside

² See proposed sections 16D-F of the Bill.

³ See, eg, proposed s 16D(1)(b).

⁴ Except in the performance of their ordinary functions and activities: see, eg, proposed s 16D(2) of the Bill.

⁵ See proposed amendments to sections 7B(1) and (2) of the Privacy Act in the Bill.

Australia will be able to access the information, but may not be subject to the jurisdiction of the Australian Privacy Act.⁶

Further information

Should the committee require any further information, please contact
Regulation and Strategy Branch

Yours sincerely

 Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

⁶ The Privacy Act does not apply extra-territorially, except where an organisation has an 'Australian link': see s 5B of the Privacy Act.