



16 December 2016

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

Dear Senator

The Digital Industry Group Inc (DIGI) welcomes the opportunity to make a submission into the Senate Legal and Constitutional Affairs Committee's inquiry on the Privacy Amendment (Re-identification Offence) Bill 2016.

DIGI comprises representatives from Google, Facebook, Twitter, Microsoft and Yahoo. DIGI members collectively provide various digital services to Australians ranging from Internet search engines and other digital communications platforms.

These services and platforms facilitate new distribution, marketing and revenue generating channels for Australian businesses and content creators. They are also driving fundamental changes to the way that business is conducted and content is created and distributed.

DIGI thanks the Committee for the opportunity to make a submission. If there are any further questions or if additional information is required, please don't hesitate to contact me.

Kind regards

Nicole Buskiewicz
Managing Director
DIGI

DIGI submission on the Privacy Amendment (Re-identification Offence) Bill

Background

DIGI and each of our member organisations are strongly committed to privacy. Our success is tied to ensuring that people have positive experiences on the platforms we provide and fundamental to this is securing and maintaining users' trust – which is key to success as an online service provider. Ultimately, it is imperative to a provider's bottom line to get users' privacy and security right. Otherwise, users will switch to a different service. This is most true in the highly competitive world of the web, where an alternative is just a click away.

We share the Government's recognition that de-identification is an important part of protecting personal data and an individual's privacy. Robust de-identification builds community acceptance and trust in the handling of their data by governments, and ensures citizens and other stakeholders continue to maintain trust and confidence in Government open data initiatives.

We also share the Government's commitment to make more public data available through open and machine readable formats on platforms such as data.gov.au. As the Productivity Commission found in its Draft Report into Data Availability and Use, the benefits of releasing de-identified government data outweigh privacy concerns. Data-driven innovation was worth \$67 billion to the Australian economy in 2013, enabling government and businesses to innovate and make fact-based decisions¹.

We have concerns, however, about whether criminalising re-identification of data is a proportionate response and we wish to make suggestions about alternate strategies that could be employed to highlight the importance of this issue.

Specific comments on the Bill

- *Requirement to notify agencies of re-identification*

The Bill provides a civil penalty provision that an entity must notify a responsible agency if the entity re-identifies de-identified personal information, whether intentionally or otherwise, and then comply with the directions from the agency about the handling of the information.

Increasingly machines, using Artificial Intelligence (AI) will engage in data matching and analytics activities with very little human interaction. Given that AI algorithms will source information from millions of publicly available datasets, it would be extremely difficult for a user to be either aware of a potential re-identification or that such analysis contained data

¹ *Deciding with data: how data-driven innovation is fuelling Australia's economic growth*, PwC report, 2014.

from an Australian Government dataset subject to the Privacy Act. DIGI is concerned that this scenario could lead to erroneous charges under the new legislation, as the onus would be on the user of these technologies to prove that they were not “aware of the re-identification”.

We are also concerned that there is no mechanism available for Government entities to notify other entities that may have inadvertently re-identified government datasets as part of broader data matching activities and published this information. We contend that the owner of the public dataset would be better placed to make a determination of whether the information has been re-identified, and it would be good to have a mechanism for the publisher to be notified and provided the opportunity to take the information down with impunity.

- *Prohibition of re-identification and disclosure of re-identified personal information*

The Bill proposes specific criminal offences and associated civil penalty provisions which provide that de-identified personal information must not intentionally be re-identified, and re-identified personal information must not intentionally be disclosed. While we share the Government’s recognition of the importance de-identification, we question the need to create a new criminal offence within the Privacy Act aimed at preventing the re-identification of de-identified data sets. In this context, a criminal offence seems unnecessarily severe, and without precedence in comparable overseas jurisdictions.

We understand that the Government’s intent is to emphasise the seriousness of de-identification processes for Government agencies, and also to protect against deliberate re-identification initiatives. However, we feel that the focus should be directed towards education, tools, technology and resources that assist agencies to ensure that data sets being publicly released are appropriately de-identified, and this de-identification has been tested and verified.

The OAIC has already produced extensive guidance for entities looking to de-identify data and we would encourage the Government to improve the usability and use of this guidance by Government entities in the release of public data.

Such an approach would further encourage community trust in government’s handling of personal information, unlike criminalising re-identification, which does little to assure the public of the robustness of the government’s de-identification processes.

- *Role of the Commissioner*

The Bill provides that once an agency becomes aware that the information is no longer de-identified, and directions for dealing with the information are given, it must inform the Australian Information Commissioner (the Commissioner). The Bill provides the Commissioner with powers to investigate the matter.

However, it may be more appropriate to require the entity to inform the Commissioner directly. We believe the Commissioner is better placed to advise on the seriousness of any potential

privacy risk, and issue directions or remedies based on the assessment. The Commissioner is also at arm's-length from any re-identification incident, and will not be incentivised to deflect responsibility for failure to effectively de-identify information in the first place, or place disproportionate blame on the re-identifying person or entity.

- Broad exceptions from the offence provisions

Specific exceptions from the offence provisions in the Bill for Federal government agencies (other than the releasing agency) are drafted in unusually wide terms:

Subsection (1) does not apply if:

(a) the entity **is an agency**; and

(b) either:

(i) the act was done in connection with the performance of the agency's functions or activities; or

(ii) the agency was required or authorised to do the act by or under an Australian law or a court/tribunal order

While the rationale for the exception is explained in the Minister's second reading speech - *'...agencies will be exempt when performing their functions or when authorised by law to ensure they can continue to perform their ordinary functions and activities such as matching a de-identified dataset to another dataset or undertaking decryption activities to test information security'* - the drafting of the exception is much broader. This seems inconsistent with the alleged severity of the consequence of re-identifying data, which according to the Bill warrants a criminal offence.