Australian Government
Attorney-General's Department

15 December 2016

Attorney-General's Department submission

Senate Legal and Constitutional Affairs Legislation Committee inquiry—Privacy Amendment (Re-identification Offence) Bill 2016

The Attorney-General's Department is pleased to provide this submission to the Senate Standing Committee on Legal and Constitutional Affairs in relation to its inquiry into the Privacy Amendment (Re-identification Offence) Bill 2016.

The Bill will provide stronger safeguards for individual privacy while supporting the Australian Government's commitment to open data and the release of de-identified public sector datasets. The aim of this submission is to provide further explanation of the policy rationale underpinning the Bill and to clarify the operation and application of particular provisions where concerns have been raised with the department to date.

Policy rationale behind the Bill

The Bill amends the *Privacy Act 1988* (the Privacy Act) to introduce provisions which prohibit conduct related to the intentional re-identification of de-identified personal information published or released by, or on behalf of, Commonwealth agencies in a generally available publication,[1] and intentional disclosure of re-identified information.[2] The Bill also introduces an obligation to notify the agency responsible for the dataset of any re-identification and to comply with any directions from that agency.[3]

The publication of government datasets, including de-identified data, enables the government, policymakers, researchers, and other interested persons to take full advantage of the opportunities that new technology creates to improve research and policy outcomes. However, public trust and confidence in the protection of privacy and personal information is an essential component of the open data agenda. The Australian Government's Public Data Policy Statement,[4] released on 7 December 2015, provides a clear mandate for agencies to optimise the use and re-use of public sector data while upholding the highest standards of security and privacy.

The Public Data Policy Statement requires Australian Government agencies to appropriately de-identify all published government data. The Office of the Australian Information Commissioner (OAIC), and several

[1] subsection 16D(1), Privacy Amendment (Re-identification Offence) Bill 2016.
[2] subsection 16E(1), Privacy Amendment (Re-identification Offence) Bill 2016.
[3] subsections 16F(3) and 16F(9), Privacy Amendment (Re-identification Offence) Bill 2016.
[4] https://www.dpmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf

privacy regulators and government bodies domestically and internationally, have recognised the value of de-identification and related statistical techniques as a way to mitigate the privacy risks of data sharing activities without irrevocably damaging the usefulness of the data.[5] It is expected that government agencies will continue to apply the highest standards in de-identification for published datasets. However, de-identification is not without risk as it is not possible to provide an absolute guarantee that de-identified information could never be re-identified. In particular, advances in technology mean methods that were sufficient to de-identify data in the past may become susceptible to re-identification in the future.

The Privacy Amendment (Re-identification Offence) Bill 2016 forms part of the Australian Government's efforts to ensure that the considerable benefits associated with the release of public sector datasets can be realised whilst upholding the highest standard of information security and protecting the privacy of Australians. Specifically, the Bill addresses an existing gap in privacy legislation to strengthen protections against re-identification within privacy legislation and act as a deterrent against attempts to re-identify de-identified personal information from published government datasets.

Other measures to ensure data is appropriately de-identified

The primary purpose of the Bill is to provide enhanced protections for de-identified personal information against re-identification, regardless of how well that information was de-identified, noting that de-identified information may become more vulnerable over time due to advances in technology. As the new offence and civil penalty provisions apply to information published by an agency 'on the basis that it was de-identified personal information',[6] the offences would also apply in situations where information has been unknowingly poorly de-identified by the agency. However, this should not be interpreted as an acceptance of poor or inadequate de-identification practices by agencies when publishing datasets.

Agencies continue to be subject to the Australian Privacy Principles (APPs) under the Privacy Act and failure to implement robust de-identification processes may risk breaching the APPs. Additionally, as noted above, the Australian Government's Public Data Policy Statement also requires agencies to appropriately de-identify all published government data. There are a number of existing resources available to assist agencies with de-identification. For example, the OAIC has published guidance material for agencies on de-identification of personal information[7] and the Australian Bureau of Statistics (ABS) has published its Confidentiality Series (available on the National Statistical Service website), which provides practical advice on confidentiality and privacy—including managing identification risks.[8]

If an agency publishes poorly de-identified personal information, the agency would potentially breach existing provisions of the Privacy Act. The Privacy Act defines de-identified information as information that is 'no longer about an identifiable individual or an individual who is reasonably identifiable'.[9] While the Privacy Act does not apply to de-identified information, if personal information has been so poorly de-identified such that it does not meet the Privacy Act's definition of 'de-identified', the Privacy Act would still apply to that information. Therefore by publishing poorly de-identified information, the agency may have breached APP 6

---

[5] https://www.oaic.gov.au/information-policy/information-policy-resources/information-policy-agency-resource-1-de-identification-of-data-and-information
[6] see paragraphs 16D(1)(b), 16E(1)(e) and 16F(1)(b), Privacy Amendment (Re-identification Offence) Bill 2016.
[7] https://www.oaic.gov.au/information-policy/information-policy-resources/information-policy-agency-resource-1-de-identification-of-data-and-information
[8] http://www.nss.gov.au/nss/home.NSF/pages/Confidentiality+Information+Sheets
[9] section 6, *Privacy Act 1988*.

of the Privacy Act (regulating use and disclosure of personal information) and APP 11 (prohibiting unauthorised access to and disclosure of personal information). In these situations, the Australian Information Commissioner would be able to use his or her existing powers under the Privacy Act to investigate whether the agency's publication of the data breached the APPs.[10] The Commissioner would also be able to use existing enforcement powers under the Privacy Act in relation to the agency's broader privacy practices.[11] For example, by making a determination that an agency take specified steps to ensure that an act or practice is not repeated or continued (such as publishing poorly de-identified personal information).[12]

To further strengthen protections for personal information, the Bill is complemented by the *Process for Publishing Sensitive Unit Record Level Public Data as Open Data* recently developed by the Department of the Prime Minister and Cabinet to govern the release of new de-identified datasets to improve processes and minimise the risk of re-identification.[13] This includes requiring the responsible agency to use a data privacy expert to develop a methodology to de-identify the dataset and a different data privacy expert to test the effectiveness of that methodology prior to releasing the dataset. The Bill also inserts new paragraph 33C(1)(f) into the Privacy Act,[14] which will provide the Information Commissioner with specific powers to undertake assessments of agency de-identification practices. This will ensure the Commissioner has oversight of agency de-identification techniques and can identify problems before they emerge. The notification requirement in section 16F of the Bill will also help ensure agencies become aware of inadequately de-identified datasets as soon as possible so that they can take appropriate steps to deal with the issue.

Retrospective operation

The offences in sections 16D and 16E apply retrospectively to conduct occurring on or after 29 September 2016.[15] The obligation to notify the responsible agency in section 16F only arises prospectively after commencement, but does apply to re-identification conduct occurring on or after 29 September 2016.[16] Retrospective offences challenge a key element of the rule of law—that laws are capable of being known in advance so that people subject to those laws can exercise choice and order their affairs accordingly. However, in the circumstances the government considers that these narrowly prescribed offences should have a limited retrospective effect.

The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* provides that offences may be made retrospective where there is 'a strong need to address a gap in existing offences, and moral culpability of those involved means there is no substantive injustice in retrospectivity.'[17] The government considers that these narrowly prescribed offences meet these requirements.

---

[10] Under existing provisions of the Privacy Act, the Commissioner has powers to assess the personal information handling practices of entities subject to the Act (s 33C), and to launch an investigation under his or her own initiative or following a complaint (s 40).
[11] At the conclusion of an investigation the Commissioner has a range of enforcement options under the Privacy Act, including accepting an enforceable undertaking (s 33E) or making a determination requiring an agency to remedy a breach of the Privacy Act or to avoid further non-compliance (s 52). Both enforceable undertakings and determinations can be enforced through the Federal Court or Federal Circuit Court in the event of non-compliance (ss 55A and 62).
[12] paragraph 52(1)(ia), Privacy Act.
[13] https://blog.data.gov.au/news-media/blog/publishing-sensitive-unit-record-level-public-data
[14] item 6, Privacy Amendment (Re-identification Offence) Bill 2016.
[15] paragraphs 16D(1)(c), 16E(1)(c) and 16E(1)(e), Privacy Amendment (Re-identification Offence) Bill 2016.
[16] paragraph 16F(1)(c) and item 21, Privacy Amendment (Re-identification Offence) Bill 2016.
[17] page 15, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.

The recently identified vulnerability in the Department of Health's Medicare and Pharmaceutical Benefits Scheme dataset brought to the government's attention the existence of a gap in privacy legislation regarding the re-identification of de-identified data. For example, the Privacy Act does not apply either to individuals acting in a personal capacity or to small businesses. In addition, the Privacy Act does not currently provide a basis to take action against individuals who re-identify de-identified data or disclose re-identified personal information. This gap will make it more likely that personal information is inappropriately released through re-identification of de-identified datasets before the Bill commences. The release of personal information can have significant consequences for individuals which cannot be easily remedied. In particular, once personal information is made available online it is very difficult—in many cases impossible—to fully retract that information or prevent further access.

Once aware of this gap, the government acted immediately to strengthen protections for personal information against re-identification by introducing these offences. The offences will only take effect in relation to conduct occurring on or after 29 September 2016, which is the day after the Attorney-General announced the proposed amendments to the Privacy Act. This retrospective application was made very clear in his statement of 28 September 2016. As a result of this statement, the community was clearly given notice that this particular conduct will be made subject to offences from that time. Further, the moral culpability of anyone covered by the Bill who intentionally re-identifies de-identified information and/or discloses re-identified information for personal or commercial gain means that there is no substantive injustice in retrospectivity.

Applying the offences to conduct occurring from the day after the Attorney-General announced the government's intention to introduce this Bill provides a strong disincentive to entities who, upon hearing of this intention, may have been tempted to attempt re-identification of any published datasets while the Parliament considers the Bill. The government has also taken action to introduce the Bill in the Parliament at the earliest available opportunity to ensure the retrospective application is for a short time period only.

Scope of offences

The offence and civil penalty provisions in the Bill have been narrowly drafted to ensure they do not inappropriately capture legitimate conduct in relation to de-identified personal information published by or on behalf of a Commonwealth agency in a generally available publication.

Firstly, the offence and civil penalty provisions only apply in relation to de-identified personal information published by, or on behalf of, a Commonwealth agency in a generally available publication, where the information was published on the basis that it was de-identified. The provisions do not apply to datasets published by private entities nor to datasets shared by an agency with a limited group of entities under a contractual arrangement or other formal agreement (which would be subject to confidentiality requirements).

Secondly, the offence and civil penalty provisions do not apply to:

- agencies in relation to acts done in connection with the performance of the agency's functions or activities or where otherwise required or authorised by law[18]

[18] see subsections 16D(2), 16E(3) and 16F(5), Privacy Amendment (Re-identification Offence) Bill 2016; note these provisions should be read together with subsection 4(2) of the Privacy Act, which provides that nothing in the Privacy Act can render the Commonwealth liable for prosecution for an offence.

- contracted service providers for Commonwealth contracts in relation to acts done for the purposes of the contract,[19] or
- entities who have entered into an agreement with the responsible agency in relation to acts done in accordance with the agreement.[20]

These exclusions ensure that entities engaged by Commonwealth agencies (under contract or other agreement) do not contravene the offence and civil penalty provisions when engaging in functions or activities for which they have been engaged—such as decryption activities to test information security. The exclusions also ensure that Commonwealth agencies do not contravene the civil penalty provisions when engaging in their ordinary functions and activities.

Thirdly, the conduct which is the subject of the offence and civil penalty provisions is narrowly confined.

The offence for re-identification in section 16D only applies to intentional re-identification of de-identified personal information. That is, the entity must have done an act with the specific intention of re-identifying the dataset.[21] Unintentional re-identification that occurs as a by-product of other public interest research using a government dataset, for example through data matching, would not constitute an offence under section 16D. While the offence for disclosure in section 16E applies to information which is intentionally or unintentionally re-identified,[22] the offence itself is confined to the intentional disclosure of re-identified information to a person or entity other than the responsible agency when the entity is aware the information is re-identified. Merely disclosing that a de-identified dataset published by government could be re-identified, or speculating about the possibility of re-identification, would therefore not constitute an offence under section 16E. Similarly, inadvertent disclosure of re-identified information where the entity is not aware that the information is re-identified would also not constitute an offence.

The department notes that the ancillary offences under the Commonwealth Criminal Code also apply to the offences in sections 16D and 16E of the Bill (similarly, section 80V of the Privacy Act, which deals with ancillary contravention of a civil penalty provision, also applies to sections 16D, 16E and 16F). These ancillary offences could include attempting, or aiding or inciting, someone to commit one of the offences contained in the Bill.[23] Ancillary offences of this kind require a link between a person's conduct and the committal of the principal offence, and the elements of these ancillary offences must be proven beyond reasonable doubt. Neither of these requirements would likely be satisfied if an entity has done nothing more than state that a government dataset is re-identifiable or theoretically vulnerable to re-identification.

The re-identification offence in section 16D reflects the position that re-identifying de-identified information is not acceptable or appropriate, except in limited circumstances where an exemption may be required (for example, in relation to public interest research involving the testing of de-identification techniques). Section 16E provides important protection against further distribution of re-identified personal information in the event it has been re-identified. Section 16F also provides important privacy protections as the obligation to notify the responsible agency that the dataset has been re-identified ensures the agency is aware of vulnerabilities in the dataset and can take appropriate steps to protect it. Section 16F applies regardless of

[19] see subsections 16D(3), 16E(4) and 16F(6), Privacy Amendment (Re-identification Offence) Bill 2016.
[20] see subsections 16(4), 16E(5) and 16F(7), Privacy Amendment (Re-identification Offence) Bill 2016.
[21] paragraph 16D(1)(c), Privacy Amendment (Re-identification Offence) Bill 2016.
[22] see subsection 16E(2), Privacy Amendment (Re-identification Offence) Bill 2016.
[23] see sections 11.1, 11.2, 11.4 and 11.5 of the *Criminal Code*.

whether the entity intentionally or unintentionally re-identified the information. This is appropriate given the privacy protecting purpose of the section. It is difficult to envisage circumstances where the prohibition against disclosure of re-identified information in section 16E and the obligation to notify the responsible agency under section 16F would interfere with the ability to conduct public interest research such that an exemption would be required.

Application to researchers

Legitimate research using government datasets should not be discouraged and it is equally important that valuable research undertaken in areas such as testing the effectiveness of de-identification techniques, cryptology or information security is able to continue. However, effective privacy and security measures protecting personal information are also necessary to ensure ongoing public confidence in open data. The department considers the provisions in the Bill strike the appropriate balance between protecting individual privacy and facilitating research.

The Privacy Act does not apply to most universities because they are established under State and Territory legislation. The proposed offence and civil penalty provisions in the Bill apply to the acts of an entity, which is defined by subsection 6(1) of the Privacy Act to include an agency, organisation or small business operator. While the proposed provisions in the Bill do have an extended application to small businesses and individuals,[24] all State and Territory authorities remain exempt—consistent with the existing position under the Privacy Act. A State or Territory authority is expressly excluded from the definition of 'organisation' in section 6C of the Privacy Act. Under subsection 16CA(2) of the Bill, this exemption also applies to acts done by individuals employed by, or engaged to provide services to, universities in the course of employment or service. It is expected that the ethical standards which apply in university research contexts will ensure that university researchers do not inappropriately re-identify government information or inappropriately handle re-identified government information.

For researchers who are not based in universities, as noted above, in addition to determinations made under section 16G, exceptions are also provided in subsections 16D(3)-(4), 16E(4)-(5) and 16F(6)-(7) for an entity who is engaged as a contracted service provider or enters into an agreement with a Commonwealth agency for research purposes, such as testing the effectiveness of de-identification techniques, in relation to acts done consistently with that contract or agreement.

Exemption determination power in section 16G

Section 16G of the Bill provides the Minister with a general power to determine that a particular entity or class of entities is exempt from one or more of sections 16D, 16E or 16F for particular purposes if it is in the public interest. This is intended to provide an appropriate balance between protecting the privacy of individuals and allowing for legitimate research to continue.

In view of the relatively narrow scope of the proposed offences noted above, and the fact that the provisions will not apply to most universities, the department does not expect there will be many entities who will require an exemption under section 16G to undertake research requiring the intentional re-identification of de-identified personal information published by a government agency in a generally available publication.

---

[24] Under the Privacy Act, individuals are captured both under the definition of 'organisation' (s 6C(1)) and the definition of 'small business operator' (s 6D(3)). Due to new subsection 16CA(1), the new offences and civil penalty provisions will apply to individuals acting in a non-business capacity.

Where an entity does wish to undertake such activities, the Minister will need to be satisfied that the 'public interest', as defined in the context of the Privacy Act, would be served by allowing the entity to perform these activities. This 'public interest' test will be a difficult test to satisfy, as re-identification actively infringes the privacy expectations of individuals whose information has only been disclosed following a de-identification process.

The power to determine that an entity is exempt for the purposes of one of more of sections 16D, 16E and 16F has been designed to provide the necessary flexibility to accommodate circumstances, not currently contemplated, which may require an exemption in the future. The Minister may grant an exemption under the 'public interest' test if it is required for specific research purposes involving cryptology, information security and data analysis, which are identified in paragraphs 16G(2)(a) to (c). Paragraph 16G(2)(d) also provides a general ground for any other purpose the Minister considers appropriate. The ability to grant exemptions for 'any other purpose' ensures there is appropriate flexibility in the event that other legitimate reasons to grant exemptions arise in the future which are not currently contemplated.

Consistent with ordinary statutory interpretation principles, subsection 16G(1) and paragraph 16G(2)(d) should be considered together with the specific research purposes identified in paragraphs 16G(2)(a) to (c). In *Hogan v Hinch* French CJ stated that when 'used in a statute, the term [public interest] derives its content from "the subject matter and the scope and purpose" of the enactment in which it appears.'[25] As protecting an individual's privacy is of upmost importance, research would generally only be in the public interest if it contributed in some way to enhancing protections for personal information (for example, testing for vulnerabilities in existing de-identification techniques or developing stronger techniques).

The department anticipates that exemptions under section 16G would generally not be required in relation to the prohibition against disclosure of re-identified information in section 16E and the obligation to notify an agency about re-identification in section 16F. It is difficult to envisage circumstances where these requirements would interfere with the ability to conduct legitimate public interest research—furthermore, as noted above, sections 16E and 16F provide important protections for individuals' privacy.

In relation to the process for making exemption determinations under section 16G, the department expects that the primary focus of any determination will be on exempting classes of entities, rather than specific individuals (although it would still be possible to exempt individual entities if required). The department intends to conduct public consultation to identify relevant classes of entities who may require exemptions prior to the Attorney-General making any determination. The department will also consider implementing a regular, annual consultation process for exemption instruments to ensure there is greater certainty and a clear process for entities which may require exemptions. As required by subsection 16G(4), the Information Commissioner will also be consulted prior to making any determination.

The department therefore considers the exemption determination power under section 16G is appropriately confined while still providing the necessary degree of flexibility.

Alternatively, if an explicit legislative exemption for legitimate research were included instead of section 16G, the department's view is that such an exemption would need to be more restrictive. This is because not all research involving data analysis or cryptology would necessarily be in the public interest. For example, research could be targeted towards hacking databases for commercial profit rather than protecting security

[25] *Hogan v Hinch* (2011) 243 CLR 506, [31].

of personal information. Very careful consideration would be required to determine the appropriate formulation for such an exemption. Furthermore, even if this approach was adopted, an 'any other purpose' exemption determination power may still be required to ensure there are no unintended consequences.

Burden of proof for exceptions

As noted above, the Bill provides for various exceptions to the offences for re-identifying de-identified personal information (subsections 16D(2) to (5)) and disclosing re-identified information (subsections 16E(3) to (6)). These exceptions are for:

- an agency where the act was done in connection with the performance of the agency's functions or activities, or the agency was required or authorised to do so by or under an Australian law
- an entity who is a contracted service provider for a Commonwealth contract to provide services to the responsible agency and the act was done for the purposes of meeting an obligation under the contract
- an entity who has entered into an agreement with the responsible agency to perform functions or activities on behalf of the agency and the act was done in accordance with the agreement, and
- an entity who is an exempt entity under a section 16G determination and the act was done for a purpose specified in the determination and in compliance with any conditions specified.

The defendant entity or agency bears the evidential burden for each of these exceptions, which reverses the criminal law principle that the prosecution must prove every element of the offence.

The Senate Scrutiny of Bills Committee has indicated that it may be appropriate for the burden of proof to be placed on the defendant where a particular matter might be said to be peculiarly within the knowledge of the defendant and/or proof by the prosecution of a particular matter would be extremely difficult or expensive to provide whereas it could be readily and cheaply provided by the accused.[26]

Requiring the prosecution to prove that the above exceptions do not apply would effectively require proof of a negative, namely that there were no applicable contracts, functions, activities, Australian laws or agreements which authorised the defendant entity or agency to engage in the conduct in question. This would be extremely difficult and expensive for the prosecution to prove beyond reasonable doubt. By contrast, this information would be readily and cheaply available from the defendant agency or entity, which would have peculiar knowledge of applicable contracts, functions, activities, Australian laws or agreements that could be used to justify their conduct. The department therefore considers this reversal of evidential burden of proof to be consistent with the principles set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.

[26] page 51, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*.