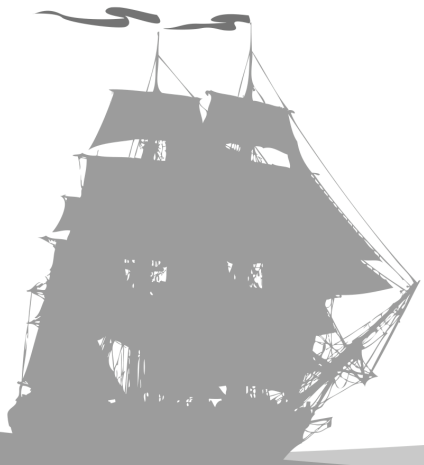
Submission to the Senate Legal and Constitutional Affairs Legislation Committee Inquiry into the Privacy Amendment (Re-identification Offence) Bill 2016 (Cth)

16 December 2016



Submission to the Senate Legal and Constitutional Affairs Legislation Committee Inquiry into the Privacy Amendment (Re-identification Offence) Bill 2016 (Cth)

William Pettersson and Tom Randle, Pirate Party Australia*

The Pirate Party thanks the Senate Legal and Constitutional Affairs Legislation Committee for the opportunity to provide a submission on the Privacy Amendment (Re-identification Offence) Bill 2016 (Cth) ('the Bill').

The Pirate Party considers Australians' right to privacy to be paramount for the health of our democracy. In that, we understand the desire to protect the privacy of Australians. However, the Bill as proposed does not protect the privacy of Australians in reality, and instead overreaches in trying to hide Government agency mistakes by criminalising those who discover badly de-identified data. While also leaving loopholes open for those who (intentionally or otherwise) actually reveal private data. The Government is attempting to create a deterrent effect on the wrong side of the debate around de-identified data, instead it is Government agencies in need of much greater restraint and deterrence from making privacy mistakes when publishing data.

As such, Pirate Party Australia thinks the legislation is completely unworkable and will not solve the stated objectives in the legislation's explanatory memorandum. The Bill should either be abandoned, completely re-worked, or referred for a thorough inquiry into the issue by a law reform body such as the ALRC[1], so that a more adequate investigation of the issues the legislation is dealing with can occur. However, if the Parliament intends to continue with this rushed legislation, our submission below goes into detail as to issues with the legislation that should be seriously considered by the Committee.

Recommendation 1: Abandon the legislation in its current form and refer the issue to a law reform body, such as the ALRC, to conduct an expert driven thorough inquiry into the issues the legislation aims to address.

*Pirate Party Australia is a federal political party registered under the *Commonwealth Electoral Act 1918* (Cth) and an incorporated association under the *Associations Incorporation Act 2009* (NSW).

[1]Australian Government, *Australian Law Reform Commission* <http://www.alrc.gov.au>.

In Section 1 we discuss the repercussions of retrospective laws, and the problems they cause. In Section 2 we point out that exceptions to government agencies seem unnecessarily broad, and recommend a more narrow wording. Section 3 points out that exceptions for acts required by law or court/tribunal order should probably extend to all entities, and not just government agencies. Section 4 closes some loopholes that exist in the Bill. Section 5 looks at the role of intent with disclosure, and the vague drafting of the legislation. Lastly, Section 6 highlights how the Bill does not grant any exceptions for public good without prior approval from the Attorney-General. We show how this can (and already has!) have a chilling effect on research in Australia which will harm data privacy research in Australia.

1 Retrospective laws and their chilling effects

The Bill introduces retrospective offences for performing acts that re-identify released data or disclose re-identified data. The presence of such retrospective offences provides a very real and very chilling effect on the free and open discourse our society requires. Given that the Bill had not been introduced (let alone discussed) in Parliament, people were unsure of exactly what would be covered by the amendments beyond the vague outline described in the Attorney-General's media release issued on 28 September 2016.[2] Indeed, even now, and despite vague assurances from the Attorney General's office, we cannot be certain exactly what would constitute an offence under the retrospective legislation. This creates an environment where many who work in data de-identification or re-identification were (and some still are) unwilling to discuss their work publicly.

It should be noted that the Attorney-General's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*[3] states:

> An offence should be given retrospective effect only in rare circumstances and with strong justification. If legislation is amended with retrospective effect, this should generally be accompanied by

[2] Attorney-General's Department (Cth), 'Amendment to the Privacy Act to Further Protect De-identified Data' (Media Release, 28 September 2016) <https://www.attorneygeneral.gov.au/Mediareleases/Pages/2016/ThirdQuarter/Amendment-to-the-Privacy-Act-to-further-protect-de-identified-data.aspx>.

[3] Attorney General's Department (Cth), *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* <https://www.ag.gov.au/Publications/Pages/GuidetoFramingCommonwealthOffencesInfringementNoticesandEnforcementPowers.aspx>.

a caveat that no retrospective criminal liability is thereby created.

Retrospective laws are prohibited under international human rights law.[4] These retrospective offences are not, as the Bill's explanatory memorandum claims, 'reasonable and necessary'.[5] There is no strong justification for these changes: data re-identification is not an unknown idea, and there has been no recent or significant increase in publicly-released data being re-identified. Although the Government did make it 'abundantly clear that it is pursuing this course of action',[6] it did not release an exposure draft of the Bill for public comment. A media release is hardly sufficient notice for researchers that their work may soon become illegal. With this in mind, and with the knowledge that those who would re-identify data with malicious intent would not publicly disclose their actions anyway, there is no reason for any retrospective effect.

Recommendation 2: All retrospective offences should be removed, the legislation and all offences therein should only commence from the day it receives Royal Assent.

2 Exceptions for agencies should only apply when required

The proposed subsections 16D(2), 16E(3) and 16F(5) provide exceptions for agencies for actions and disclosures made 'in connection with the performance of the agency's functions or activities'. This provides an unreasonably broad and vague exception. An agency's functions or activities would often include publishing data, and it is easily argued that there is a connection between an act intended to release de-identified personal information, and the act which mistakenly releases the related identifiable personal information.

[4] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 172 (entered into force 23 March 1976) art 15.

[5] Explanatory Memorandum, Privacy Amendment (Re-identification Offence) Bill 2016 (Cth) 9.

[6] Ibid.

Recommendation 3: Amend the Bill so that the exceptions in sub-paragraphs 16D(2)(b)(i), 16E(3)(b)(i) and 16F(5)(b)(i) will only apply if the performance of the agency's function or activities actually requires the publication of de-identified data.

3 Acts required by law or court/tribunal order

Agencies are given explicit exceptions if required or authorised by or under 'an Australian law or court/tribunal order' to perform an act or disclose information. There is no reason this exception need only apply to agencies.

Recommendation 4: Allow the exceptions listed in the proposed sub-paragraphs 16D(2)(b)(ii), 16E(3)(b)(ii) and 16F (5)(b)(ii), which permits acts and disclosures required or authorised by Australian law or court/tribunal orders, to apply to all entities (including individuals), not only government agencies.

4 Close loopholes from Commonwealth contracts or agreements

The proposed subsections 16D(3)–(4), as well as 16E(4)–(5) and 16F(6)–(7), provide exceptions to entities working under either a Commonwealth contract, or an agreement with the responsible agency. In cases where any of these subsections apply, any act which re-identifies data, or publicly discloses data which is no longer de-identified, does not have any consequence. This is at odds with the intended objects of this Act. If the act was done for the purpose of meeting an obligation, but was not specifically required, then subsections 16D(1), 16E(1) and 16F(1) should still apply. As it stands, there is a break between the purpose of the Bill and its outcome. This loophole should also be closed.

Recommendation 5: Replace the word 'done' with the word 'required' in paragraphs 16D(3)(b), 16D(4)(b), 16E(4(b), 16E(5)(b), 16F(6)(b) and

16F(7)(b).

This still leaves out cases where the act was required for meeting an obligation. In such cases, subsections 16D(1), 16E(1) and 16F(1) would still not apply, even if re-identified personal information is released without reason. It would be more suitable in such cases to re-assess the act as if it were taken by the agency responsible for the Commonwealth contract and/or agreement.

Recommendation 6: Amend the proposed sections 16D, 16E and 16F to include a provision that if an entity was required to perform an act under a Commonwealth contract or agreement by an agency, the act shall be taken to have been performed by the agency.

5 Intent and disclosure

The proposed subsection 16E(1) creates an offence for disclosing re-identified data derived from de-identified data, regardless of whether there was any intention to de-identify the data. The drafting of the provision leaves some aspects vague. In particular, it is unclear whether the entity needs to be aware *at the time of disclosure* that the data is no longer de-identified. This leaves it ambiguous as to whether the disclosure of information that the entity later learns is re-identified would be considered a contravention of this subsection.

Recommendation 7: Replace paragraph 16E(1)(d) and 16E(1)(e) with:

> (d) on or after 29 September 2016, the entity discloses the information to a person or entity other than the responsible agency; and
>
> (e) at the time of the disclosure the entity is aware that the information is no longer de-identified.

Even ignoring this vague drafting, the proposed section 16E is still unreasonably heavy-handed. By discussing published de-identified personal inform-

ation, an entity can easily be seen as disclosing said information. If only through such a discussion, a third party is then made aware of the information and re-identifies it, then the act by the original entity is one which resulted in the information no longer being de-identified, even though no intent was present. Such possibilities extend to any public discussion of released information, and could easily stifle said public discussion.

Recommendation 8: Replace the proposed subsection 16E(2) with:

> Paragraph (1)(c) applies if the entity would have a reasonable expectation that the act would have the result that the information is no longer de-identified.

The Bill would make it an offence to disclose the re-identification of personal information. However, it provides no timeline for any sort of authoritative response from the responsible agency. If personal information is leaked, those affected have a right to know. An agency can retract published information, and take any mitigating steps it deems appropriate, in a short amount of time. If an entity discloses the re-identification of data, then the agency responsible should be given a short time to resolve the issue as best as possible. After this time has lapsed, the original entity should be free to publicly disclose that published information by the agency can be re-identified.

Recommendation 9: At the end of paragraph 16E (6) insert:

> (6A) Subsection (1) does not apply if:
>
> (a) the entity has notified the responsible agency in accordance with section 16F; and
>
> (b) more than 7 days have passed since said notification.

6 Exceptions for public good

The Bill contains no explicit exceptions for any research or other work into re-identification for the public good. Although the proposed section 16G does give the Attorney-General the authority to determine that an entity is an ex-

empt entity for the purposes of the legislation, this in itself does not grant any exceptions. There is no guarantee that the Attorney-General *must* consider granting any such exception to an entity working for the public good. Even if the Attorney-General were to consider granting such an exception, there is no guarantee that an exception would be granted, even if it could be demonstrated that the act was in good faith, had no negative consequences and was in the interest of the public good. The recent disputes between the Attorney-General and former Solicitor-General Justin Gleeson SC highlight the fact that these roles are occupied by people who do have personal biases, and who have made mistakes. This extension of executive government powers is also to be questioned, the legislation in attempting to resolve its stated purpose in law is actually granting new powers to the executive government, something which ordinarily should not be done without solid justification which appears deficient.

Recommendation 10: To avoid biased decision-making, the legislation should specifically require that any public benefit be considered for any act to which the legislation might apply. This should specifically require (but not be limited to) considering the desired outcome of the entity performing the act, the steps (if any) taken by the entity to attempt to safeguard personal information, and whether the actual outcomes of the act were in the public good.

As phrased, the Bill would have a chilling effect on any research in data re-identification. The Bill does not give any significant protection to researchers who have not already been granted exceptions. The threat of significant fines and possible jail time is likely to greatly reduce the amount of research in this area, and do more harm than good to the public. If a researcher discovers a method of re-identifying data, but is unaware that there exists some published data which is vulnerable to this new technique, the researcher should not be punished. The onus should lie with the responsible agency to stay current in the field of re-identification regarding any data it has published. This is especially true as the legislation will obviously not apply to researchers around the globe, so any responsible agency should already be following the research in the field.

Recommendation 11: The Bill should specifically exclude any act which, on its own, is only research in the field of re-identification (unless

the research specifically links to a vulnerable dataset and the responsible agency is not notified under section 16F).