Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

16 December 2016

Senate Legal and Constitutional Affairs Legislation Committee

By email: legcon.sen@aph.gov.au.

Dear Committee Secretary,

Re: PRIVACY AMENDMENT (RE-IDENTIFICATION OFFENCE) BILL 2016

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

This submission by the Australian Privacy Foundation responds to the Privacy Amendment (Re-identification Offence) Bill 2016 ("the Bill"), referred to the Senate Legal and Constitutional Affairs Legislation Committee on 10 November 2016.

The Australian Privacy Foundation (APF) supports measures that improve privacy protection in Australia. In particular, the APF shares widespread concerns about the privacy-invasive implications of re-identification technologies. However, the proposed offences contained in the Bill are an inadequate response to underlying, intrinsic vulnerabilities associated with current de-identification methods which have the potential for re identification of personal information as re-identification becomes feasible. The proposed law is misconceived as blunt criminal prohibitions will inhibit legitimate data security research, including research into de-identification and re-identification technologies.

The process associated with the introduction and proposed passage of the Bill is cause for concern. It was hurriedly prepared and introduced, presumably in response to several dramatic instances where supposedly de-identified data sets, published in the public domain under the rubric of 'Open Data (including Medicare 10% sample and a public servant census) were re-identified with relative ease. This occurred despite claims of effective anonymisation. It is relevant to note that these breaches of established de-identification precautions were done for research purposes and were deliberately drawn to public attention. It is the fact that it these instances of re-identification are publicly known which has caused the controversy. The controversy, and likely embarrassment, seems to be the genesis of this supposedly urgent but inadequate and flawed response. It is almost certain that the same data sets, and many others released with similarly unreliable protection, could be breached again by anyone, anywhere, and at any time into the future. However with such a prescriptive regime as envisaged by the Bill the difference would be that the public would probably not be told of the breach, and it would not be detected or even detectable.

The concern and haste seems to be less about the risks of re-identification, which have long been known, and more about the sudden embarrassing publicity that predictably revealed 'the de-identification emperor has no clothes'.

This haste (and failure to investigate options in depth) is in marked contrast to the deep lack of urgency in legislating for the more significant privacy protections that would give individuals some basis for confidence that their data is safe, that it is recognised as a source of risk, and that those responsible would be held to account if it is breached. For instance, the mandatory data breach notification bill, still not passed, is both weak and inadequate and would be made even more ineffective if it excludes data breach by de-identification. It would effectively then be useless against this growing global threat. A statutory tort of serious intrusion of privacy has been recommended numerous times since 2008 yet legislative action has not been forthcoming despite calls by states, courts and reviews.

The APF has the following specific concerns regarding the Bill:

- the capacity for re-identification of de-identified data sets is increasing, both in Australia and in other countries, where such data will most likely be published. Existing and established methods of de-identification are increasingly becoming vulnerable to 'brute force' Big Data analytic tools and machine learning/Artificial Intelligence, and to cross-referencing against the expanding body of data sets accessible in the cybersphere, including those sets deliberately published, those hacked, and those accessible via commercial or government methods. Recent work by researchers at National ICT Australia ("NICTA"), and in other countries, suggests that protection from various methods of re-identification by obfuscation or similar existing methods will decline steadily over time. As such it may be a question of when, not if, re-identification of a given data set becomes feasible. In that regard Bruce Schneier, a respected IT security authority, has suggested that personal or sensitive data becoming vulnerable to the rapid onslaught of hacking and re-identification successes will come to be seen as a 'toxic asset' rather than a safely exploitable commodity. The Bill does little to address this issue.

- as a relevant example, the Government is increasingly using a Statistical Linkage Key (SLK) to store personal information obtained from a vast range of social services (from health to a range of community services). The SLK is formed by part of the last name, part of the first name, date of birth and gender. It is trivial to re-identify the personal information in some circumstances. As a consequence, personal information is at real risk of re-identification. If the SLK's were ever released then this would be an enormous data breach. The proposed Bill would not assist the victims of that breach in any way. It is fundamental to ensure that data security and privacy in this environment incorporates a '**data minimization'** approach, whereby personal data is only collected if absolutely necessary. The collection of any data inherently poses data breach risks – and thus privacy risks. If the Australian Government and Parliament view data security and data privacy as of the utmost importance, it is incumbent that they legislate strong rules mandating data minimization. The combination of over-confidence in de-identification techniques, which encourages a de facto 'collect it all, release it all' strategy, together with ineffective prohibitions on re-identification will result in a continuing policy failure.

- a criminal offence of re-identification proposed in the Bill, is an ineffective response because:

    - there is no evidence that making re-identification a criminal offence would actually prevent the conduct. In fact, it seems unlikely that such an offence would influence the behaviour of nefarious actors in this arena.

    - it applies 'after the horse has bolted' approach to regulation. That is the antithesis of an effective risk minimisation strategy beforehand. It is like holding up your hand

against the incoming tide and commanding it to stop, rather than building a breakwater.

- it excludes, by law, government entities that do re-identification. There is existing capacity to do data matching where that is justified and properly overseen, so there is no justification for a blanket exemption.

- it is likely to be ineffective in that most re-identification is undertaken outside of Australia. It is very difficult to apply Australian laws against an activity that is becoming trivially easy and commercially incentivised around the world.

- it may also exclude all those re-identification efforts which do not come to notice, because the scale, intrusiveness and resources for investigation and prosecution efforts necessary to identify all or even most re-identifications will not be justified as against the many other abuses the criminal law system covers. Re identification is relatively be easy to do, easy to hide, and easy to move offshore. It is correspondingly expensive and prohibitively time intensive to find, where possible.

- We are also concerned about the 'whitelist' approach incorporated into the Bill permitting some entities to undertake data security work that may involve government data being re-identified. This vests too much power in the Attorney-General to approve or disapprove of entities conducting data security work.

- we are concerned about how this measure may penalize Australian-based data security researchers.

- as noted above, the proposed law will be inapplicable in practice to entities operating overseas who may be able to re-identify Australian government data released publicly. The offences proposed in the Bill will not be (easily) enforceable against them. Such entities include counterparts or competitors of Australian researchers, commercial data miners, foreign intelligence agencies, individuals, and various hacking operations.

- these measures are a risky policy experiment internationally, given no other jurisdiction comparable to Australia has any similar laws currently in place. We note that the Explanatory Memorandum mentions the UK is considering similar measures, but it has not implemented them so far. (It has also shown a remarkable hostility to effective digital privacy and personal information security protection in recent months.) The lack of international experience amplifies our concerns about the negative effects these measures may have on data security research in Australia.

- these measures do not provide any incentives for Australian government agencies to increase their data security, or investigate and adopt data minimisation, nor for researchers to announce a vulnerability or breach, and instead will operate on a 'shoot the messenger' basis by targeting those who re-identify data.

- we consider that people who find vulnerabilities in de-identified data including possible re-identification should be able to communicate this publicly and not just to the government agency in question (which may have no incentive to reveal publicly that its methods are flawed or that its assurances of safety to data subjects are no longer reliable) The general public should be made aware of the vulnerabilities of de-identification technologies at the earliest possible time so they can can take prompt measures to protect their own data security and privacy. The reflexive secrecy of many federal agencies today is not conducive to public data safety.

- there is no requirement on agencies who release or give access to data which is subsequently re-identified:

- to be held responsible for release, no matter how uninformed, negligent or incompetent;
- to conduct long term global audits and checks to determine if a once-protected data set has been re-identified anywhere;
- to notify individuals if their data is breached; or
- to carry out long term research and monitoring of the gradual erosion of de-identification effectiveness in the real world predicted by researchers.
- They would be also exempt from even the limited protection of the bill, if they were themselves to engage in re-identification. This undermines a culture which is proofed against re-identification.

Given that the data custodians are the proper locus of control and responsibility (since those breaching a re-identification ban will be elusive, and data subjects have no rights in this process), this is a major flaw. This approach of letting those who create the risk off the hook offers no prospect of encouraging the respectful approach to the risk of re-identification that is needed. 'All care but no responsibility' is not the right approach here.

- it also gives no protection, information, remedy, role or control to those individuals whose data is negligently or incompetently released, treating them as passive victims who have no option but to submissively accept their fate as agencies project future risk onto them. (In most cases they will not even be witnesses to any offence committed, so they would have no role in the criminal process.)

Instead of this Bill, the Australian Government and Parliament should adopt a range of privacy-protective measures, including:

- introduce tougher data and personal information security measures and practices in the form of legislation for Australian government agencies and private sector entities, rewarding discovery of weaknesses in protection and creative 'data minimisation' strategies, with strong penalties for these organisations in the event of data breaches.
- prioritise areas of privacy protection for governmental and parliamentary action, including:
  - the introduction of data minimization rules;
  - the tort for serious invasion of privacy;
  - compensation for breaches of privacy and effective access to justice to obtain that compensation
  - amend and strengthen the proposed mandatory data breach notification Bill (including ensuring that data breach by re-identification is covered as a 'breach', rather than potentially being left out); and
- undertake a comprehensive review of the privacy implications of emerging commercial and government practices, including re-identification technologies and Big Data analytics, including the implications of ongoing reduction over time in the protection afforded by existing de-identification methods in the face of constant advances in these areas.

An inquiry into the growing future unreliability of de-identification measures (and thus the vulnerability of every data set released under a protection which is later breached) is a

necessary step on the path to a more robust response to the risk of re-identification. There is potential that a hastily developed, ineffective criminal offence becomes a token gesture that will distract from the real task: that of properly identifying the nature of the risks that will be projected onto individuals by weakly de-identified publication or access, and developing the sort of response that could effectively deal with them.

Thank you for your consideration.

Yours sincerely

Kat Lane, Chair

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, Subcommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Subcommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html

- The Media (2007-) http://www.privacy.org.au/Campaigns/Media/