

The Senate

Legal and Constitutional Affairs
Legislation Committee

Privacy Amendment (Re-identification
Offence) Bill 2016

February 2017

© Commonwealth of Australia 2016
ISBN 978-1-76010-509-9

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.



The details of this licence are available on the Creative Commons website: <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

This document was produced by the Senate Legal and Constitutional Affairs Committee secretariat and printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

Members of the committee

Members

Senator the Hon Ian Macdonald (LNP, QLD) (Chair)

Senator Louise Pratt (ALP, WA) (Deputy Chair)

Senator David Fawcett (LP, SA)

Senator Nick McKim (AG, TAS)

Senator Linda Reynolds (LP, WA)

Senator Murray Watt (ALP, QLD)

Participating Member

Senator Derryn Hinch (DHJP, VIC)

Secretariat

Ms Toni Matulick, Committee Secretary

Ms Pothida Youhorn, Principal Research Officer

Ms Jo-Anne Holmes, Administrative Officer

Ms Margaret Jones, Administrative Officer

Suite S1.61

Parliament House

CANBERRA ACT 2600

Telephone: (02) 6277 3560

Fax: (02) 6277 5794

Email: legcon.sen@aph.gov.au

Table of contents

Members of the committee	iii
Chapter 1	1
Introduction	1
Referral	1
Background and purpose of the bill	1
Overview of the provisions of the bill.....	2
Financial implications	4
Compatibility with human rights and freedoms	4
Conduct of inquiry.....	4
Structure of this report.....	4
Acknowledgements	4
Chapter 2	5
Key issues	5
Releasing de-identified information	5
Criminalising re-identification of data	6
Scope of offences and civil penalties	8
Breadth of the Minister's discretionary power to exempt	11
Retrospectivity.....	13
Reverse burden of proof	16
Committee View.....	18
Dissenting Report of the Australian Labor Party and Australian Greens .	21
Appendix 1	23
Public submissions	23
Answers to questions on notice	23

Chapter 1

Introduction

Referral

1.1 The Privacy Amendment (Re-identification Offences) Bill 2016 (the bill) was introduced into the Senate on 12 October 2016 by the Attorney-General, Senator the Hon George Brandis QC.¹ On 10 November 2016, the Senate referred the bill to the Senate Legal and Constitutional Affairs Legislation Committee for inquiry and report by 7 February 2017.²

Background and purpose of the bill

1.2 In December 2015, the Prime Minister, the Hon Malcom Turnbull MP, released the *Australian Government Public Data Policy Statement*, which recognised that data held by the Australian Government is a national resource and noted its importance for the growing economy, improving service delivery, and transforming policy outcomes for Australia.³ The Prime Minister committed the Australian government to, as a default, make publicly available non-sensitive data to allow the private and research sectors to also benefit from the data. In releasing information, the government recognised the importance of effectively managing the data and 'upholding the highest standard of security and privacy for the individual, national security and commercial confidentiality'.⁴

1.3 In line with the Public Data Policy Statement, the Attorney-General announced on 28 September 2016 amendments to the *Privacy Act 1988* (Privacy Act) to strengthen the protections of data published by the Australian government:

In accepting the benefits of the release of anonymised datasets, the Government also recognises that the privacy of citizens is of paramount importance.

...However, with advances of technology, methods that were sufficient to de-identify data in the past may become susceptible to re-identification in the future.

The amendment to the Privacy Act will create a new criminal offence of re-identifying de-identified government data...

1 *Senate Hansard*, 12 October 2016, p. 1640.

2 *Journals of the Senate*, No. 15, 10 November 2016, p. 448.

3 The Hon Malcom Turnbull MP, Prime Minister, *Australian Government Public Data Policy Statement*, 7 December 2015, p. 1.

4 The Hon Malcom Turnbull MP, Prime Minister, *Australian Government Public Data Policy Statement*, 7 December 2015, p. 2.

The legislative change, which will be introduced in the Spring sittings of Parliament, will provide that these offences will take effect from today's announcement.⁵

1.4 In his second reading speech, the Attorney-General explained that the publication of major datasets is an important part of 21st century government, and of the government's Digital Transformation Agenda.⁶

1.5 In response to a request from the Senate Standing Committee for the Scrutiny of Bills, the Attorney-General provided further explanation for this bill:

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. Once aware of this gap, the Government acted immediately to strengthen protections for personal information against re-identification by introducing these offences.⁷

Overview of the provisions of the bill

1.6 The scope of the bill is limited to personal information which has been de-identified by an agency and is generally made available. The bill, if passed, would operate retrospectively and prohibit intentional conduct by an entity that occurred from 29 September 2016 which:

- re-identifies personal information that was de-identified by the responsible agency (proposed subsection 16D(1)); or
- discloses the re-identified personal information (proposed subsection 16E(1)).

1.7 An entity that contravenes the above provisions may be subject to a criminal penalty of up to two years imprisonment or 120 penalty units, or a civil penalty of 600 penalty units.

1.8 Additionally, regardless of the intentions of the entity, where de-identified personal information has been re-identified, the entity must notify the responsible agency that the information is no longer de-identified, cease any use or disclosure of the re-identified information, and comply with the directions of the agency about the handling of the information (proposed section 16F). The entity may be subject to a civil penalty of up to 200 penalty units for failing to notify the responsible agency in writing, or for using or disclosing the information after it becomes aware that the information is no longer de-identified (proposed subsections 16F(3) and (4)).

5 Senator the Hon George Brandis QC, Attorney-General, 'Amendment to the Privacy Act to further protect de-identified data', *Media release*, 28 September 2016. www.attorneygeneral.gov.au/MediaReleases/Pages/2016/ThirdQuarter/Amendment-to-the-Privacy-Act-to-further-protect-de-identified-data.aspx (accessed 29 November 2016).

6 Senator the Hon George Brandis QC, Attorney-General, *Senate Hansard*, 12 October 2016, p. 1642.

7 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 671.

1.9 Transitional arrangements exist for proposed section 16F so that an entity that becomes aware that de-identified information has been re-identified on or after 29 September 2016 and prior to the commencement of this item, must notify the responsible agency as soon as practicable after the commencement of this item (item 21).

1.10 While the Privacy Act is generally limited to agencies, the bill applies to organisations, small businesses and individuals (proposed section 16CA). The Explanatory Memorandum (EM) explains that the broader scope of the bill is necessary 'due to the need for a general deterrent to the re-identification of de-identified personal information'.⁸

1.11 The bill provides some exclusions which enable entities to continue to engage in their ordinary functions and activities. Specifically, the bill does not apply to agencies, Commonwealth contracted service providers and entities that enter into agreements with agencies if re-identification or disclosure:

- was done in connection with the agency's functions or activities or was required or authorised to be done by or under Australian law (proposed subsections 16D(2), 16E(3) and 16F(5));
- was done for the purposes of meeting (directly or indirectly) an obligation under a Commonwealth contract (proposed subsections 16D(3), 16E(4) and 16F(6)); and
- was done for the purposes of an agreement with the agency (proposed subsections 16D(4), 16E(5) and 16F(7)).

1.12 Additionally, the bill reverses the evidentiary burden of proof so that entities are required to show that the re-identification or disclosure was done in connection with one of the exclusions as outlined above.

1.13 The bill provides for the Minister, following consultation with the Australian Information Commissioner (the Commissioner), to make a determination to exempt an entity from the offences and civil penalties on the basis of public interests (proposed section 16G). While the Minister's determination is a legislative instrument it is not subject to disallowance under section 42 of the *Legislation Act 2003*.

1.14 The bill proposes amendments to the Commissioner's functions and powers which enable the Commissioner to conduct an assessment of whether methods used by agencies for de-identifying personal information are effective to protect individuals from being identifiable or reasonably identifiable (item 6). The bill also confers powers on the Commissioner to investigate actions relating to the re-identification of personal information which was de-identified, make determinations in relation to the investigations, and require an entity to comply with such determinations (proposed subsection 40(2A)).

8 Privacy Amendment (Re-identification Offence) Bill 2016, Explanatory Memorandum (EM), p. 18.

Financial implications

1.15 The EM notes that the bill has no significant impact on Commonwealth expenditure or revenue.⁹

Compatibility with human rights and freedoms

1.16 The EM states that the bill engages in various rights and freedoms expressed in the *International Covenant on Civil and Political Rights* (ICCPR), including the right to privacy, the right to freedom of expression, the right to a fair trial, and the prohibition on retrospective criminal laws.¹⁰ The bill's compatibility with human rights and freedoms will be discussed in chapter two of this report.

Conduct of inquiry

1.17 In accordance with usual practice, the committee advertised the inquiry on its website and also wrote to organisations and individuals inviting written submissions by 16 December 2016. The committee received 15 submissions, listed at Appendix 1. The committee also sought additional clarification on particular provisions of the bill from the Attorney-General's Department.

Structure of this report

1.18 This report consists of two chapters:

- Chapter 1 outlines the background and provides an overview of the bill, including the administrative details of the inquiry.
- Chapter 2 sets out the key issues raised in submissions, and provides the committee's views and recommendation.

Acknowledgements

1.19 The committee thanks all submitters to this inquiry.

9 EM, p. 3.

10 EM, pp. 5–9.

Chapter 2

Key issues

2.1 During the course of this inquiry a number of key issues concerning the Privacy Amendment (Re-identification Offence) Bill 2016 (the bill) were raised with the committee. These issues include:

- releasing de-identified information;
- criminalising the re-identification of data;
- scope of the offences, including the entities captured by the offences;
- scope of the Minister's discretionary power to exempt;
- retrospectivity of the bill; and
- reversed burden of proof.

2.2 This chapter will outline the above issues raised by submitters, and provide the committee's views and recommendations on the bill.

Releasing de-identified information

2.3 Submitters generally expressed their support for the bill's objective of providing greater protection to an individual's privacy. However, some submitters raised concerns that the bill would not necessarily achieve its policy goals. One submitter questioned whether personal de-identified information should be made public as the risk of re-identification may be too great.¹ A number of submitters also highlighted that it may not be possible to truly de-identify information in light of continuing advances in technology:

With more and more aspects of individual's lives involving some aspect of online interaction, and the increasing sophistication of data-mining technologies, the likelihood that even carefully de-identified data sets can be re-identified is also increasing.

It is therefore likely that not even the most expertly de-identified data sets will remain un-re-identifiable indefinitely.²

2.4 The government has outlined its view that the benefits of open data outweigh the risks of re-identification. This view was shared by the Productivity Commission in its draft report *Data Availability and Use*. This report stated that the risks of re-identification of data and harm to an individual were real and should not be trivialised, however noted that many of these risks could be managed with the right policies and processes.³ The report also noted that increasing data use does not necessarily put individuals at a greater risk of harm.⁴ It concluded that Australia

1 Mr Justin Warren, *Submission 2*, p. 2.

2 Electronic Frontiers Australia, *Submission 14*, p. 2.

3 Productivity Commission, draft report, *Data Availability and Use*, October 2016, pp. 8–9.

4 Productivity Commission, draft report, *Data Availability and Use*, October 2016, p. 11.

stands out among other developed countries where information, particularly in the area of health, is poorly used and suggested that fundamental change was needed with the introduction of new legal and policy frameworks.⁵ These frameworks would work towards four key elements:

- giving individuals more control over data held about them;
- encouraging and enabling broad access to government datasets;
- increasing the usefulness of publicly funded identifiable data among trusted users; and
- creating a culture where non-personal and non-confidential data is released as a default.⁶

2.5 The Office of the Australian Information Commissioner (OAIC) agreed that a careful balance is needed between open data and privacy protections and warned that the bill, in and of itself, would be unlikely to eliminate the privacy risks associated with the publication of de-identified datasets.⁷ OAIC outlined the need to consider whether the risk of re-identification is sufficiently low for the data to be published 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.⁸

Criminalising re-identification of data

2.6 Some submitters raised concerns that to criminalise conduct relating to re-identification was not proportionate to other offences within the Privacy Act, which generally attracts civil penalties.⁹ The Law Council of Australia (LCA) noted that the introduction of criminal sanctions was 'potentially disruptive and unworkable'.¹⁰

2.7 The Attorney-General's Department (AGD) outlined that the Privacy Act already contains a number of criminal offences in the credit reporting context, as well as for failure to attend a conference when directed by the Australian Information Commissioner.¹¹ However, it has been noted that these offences 'are arguably exceptional' to the Privacy Act, with the Australian Law Reform Commission having

5 Productivity Commission, draft report, *Data Availability and Use*, October 2016, pp. 5–6, 12.

6 Productivity Commission, draft report, *Data Availability and Use*, October 2016, p. 12.

7 Office of the Australian Information Commissioner (OAIC), *Submission 5*, p. 1.

8 OAIC, *Submission 5*, p. 2.

9 Australian Bankers' Association Inc., *Submission 15*, p. 1, and DIGI, *Submission 8*, p. 3.

10 Law Council of Australia (LCA), *Submission 10*, p. 7.

11 Attorney-General's Department (AGD), answers to questions on notice, 19 January 2017 (received 25 January 2017). Refer to ss 20P, 21R and 46 of the *Privacy Act 1988*.

previously recommended that the credit reporting offences be repealed and replaced with civil penalties.¹²

2.8 The AGD explained the rationale for the criminal penalties within the bill in the following way:

...de-identification of data is not without risk as it is not possible to provide an absolute guarantee that de-identified information could never be re-identified. The Government needs to balance this risk against the public benefit that the release of de-identified data presents. Accordingly, the Bill provides for re-identification offences at sections 16D and 16E as they are an appropriate mechanism to deter entities from doing considerable harm by re-identifying and/or disclosing re-identified personal information.¹³

2.9 Other submitters expressed a view that it is inequitable to criminalise conduct relating to the re-identification of data but not to criminalise conduct relating to poorly or improperly de-identified data. It was argued that the harm would be caused by the publication of the poorly de-identified dataset by the responsible agency and not by the entity that notices that the dataset has been poorly de-identified.¹⁴

2.10 The AGD explained that agencies are already subject to the Australian Privacy Principles (APPs) under the Privacy Act and failure to implement robust de-identification processes may risk breaching the APPs.¹⁵ In broad terms, the APPs are a set of principles concerning the handling, use and management of personal information and these apply to Australian government agencies, private health service providers, the private sector and not-for profit organisations with an annual turnover of more than \$3 million and some small businesses. Under APP 1.2, agencies are required to implement practices, procedures and systems to ensure that they comply with the Privacy Act, which includes taking reasonable steps to ensure that personal information is not disclosed through open publication.¹⁶

2.11 To assist agencies to properly manage and de-identify data increasing numbers of Commonwealth resources are being made available. This includes guidance developed by the OAIC,¹⁷ the Australian Bureau of Statistics,¹⁸ and the

12 Mary Anne Neilsen, Privacy Amendment (Re-identification Offence) Bill 2016, *Bills Digest No. 55, 2016–17*, Parliamentary Library, Canberra 2017, p. 14.

13 AGD, answers to questions on notice, 19 January 2017 (received 25 January 2017).

14 Mr Justin Warren, *Submission 2*, p. 2.

15 Attorney-General's Department (AGD), *Submission 6*, p. 2.

16 OAIC, *Submission 5*, p. 2.

17 OAIC, *Information Policy Resource 1: De-identification of data and information*, April 2014, and *Privacy business resource 4: De-identification of data and information*, April 2014.

18 Australian Bureau of Statistics, *Sheet 3 – Confidentiality: Managing identification risks*, www.nss.gov.au/nss/home.nsf/NSS/D216458568555BF4CA2579330018F598?opendocument (accessed 23 January 2017).

Department of the Prime Minister and Cabinet.¹⁹ Additionally, the OAIC is in the process of updating its de-identification guidance materials and advises that it expects these resources to be released for consultation by early 2017.²⁰

2.12 As a way of strengthening the ability of Commonwealth agencies to manage privacy risks the OAIC suggested the development of a Privacy Code across the Australian public sector.²¹ The OAIC explained that a Privacy Code could set out how one or more of the APPs are to be applied and impose additional requirements to those contained in the APPs, thereby supporting agencies towards best de-identification practices.²²

Scope of offences and civil penalties

2.13 Submitters were broadly concerned with two aspects relating to the scope of the offences and civil penalties proposed in the bill: the entities that would be captured by the new provisions; and that the provisions were drafted too broadly.

Entities captured

2.14 It is noted that the bill has a wider reach than the Privacy Act as, in addition to applying to Australian government agencies and private sector organisations, it also applies to small businesses²³ and individuals acting in their private capacity. The bill has exclusions which apply to agencies in connection with the performance of their functions and activities, contracted service providers for the purpose of meeting an obligation under a Commonwealth contract, and entities for the purpose of an agreement with the agency.

2.15 A number of submitters were particularly worried that researchers would be captured by the bill and that this would have the effect of discouraging investigation and research into information security.²⁴ One submission suggested that the effect of criminalising re-identification of data would be to:

19 Department of the Prime Minister and Cabinet, *Process for publishing sensitive unit record level public data as open data*, December 2016, https://blog.data.gov.au/sites/g/files/net626/f/process_for_publishing_open_data_dec16.pdf (accessed 23 January 2017).

20 OAIC, *Submission 5*, p. 1.

21 OAIC, *Submission 5*, p. 2.

22 OAIC, *Submission 5*, p. 2.

23 'Small business' is defined in s 6D of the Privacy Act as a business with an annual turnover of \$3 million or less.

24 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 3; Rosie Williams, *Submission 4*, p. 1; Dr Peter Ansell, *Submission 3*, p. 4; Electronic Frontiers Australia, *Submission 14*, p. 3; and Australian Bankers' Association Inc., *Submission 15*, p. 2.

...inhibit open investigation, which could mean that fewer Australian security researchers find problems and notify the government. Criminals and foreign spy agencies will be more likely to find them first.²⁵

2.16 The Explanatory Memorandum (EM) explains that proposed subsection 16CA(2) makes clear that an entity that is employed by, or engaged to provide a service to, a State or Territory authority is exempt from the operation of the Privacy Act.²⁶ The OAIC explains 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.²⁷

2.17 However, some submitters remain concerned that the bill may continue to bind State and Territory authorities which could capture universities and researchers employed by universities.²⁸ The Attorney-General has reiterated that State and Territory authorities, which includes universities, are not subject to the Privacy Act and therefore also not subject to the offences and penalties of the bill:

I note that the provisions in the Bill do not apply to universities or any other authorities established under State and Territory authorities (see subsection 6C(1) of the Privacy Act, which states that an organisation for the purposes of the Privacy Act does not include a State or Territory authority): Under subsection 16CA(2) of the Bill this exemption also applies to acts done in the course of employment or service by individuals employed by, or engaged to provided services to, those exempt universities...²⁹

2.18 Two submitters expressed a view that researchers should not need to be affiliated with a university or institution to fall outside of the scope of the bill and claimed that their work in the area of cyber security would be stifled due to the provisions of the bill.³⁰

25 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 1.

26 Privacy Amendment (Re-identification Offence) Bill 2016, Explanatory Memorandum (EM), p. 12.

27 OAIC, *Submission 5*, p. 3.

28 NSW Office of the Privacy Commissioner, *Submission 13*, p. 2.

29 Attorney-General's response, Senate Standing Committee for the Scrutiny of Bills, *Tenth report of 2016*, 30 Nov 2016 p. 668.

30 Mr Andrew van der Stock, *Submission 7*, p. 3; and Mercury Information Security Services, *Submission 9*, p. 1.

2.19 The Attorney-General explained that the offences created under the proposed sections of the bill would be unlikely to interfere with the ability to conduct research which is in the public interest.³¹ The AGD outlined that for those researchers who were not based in universities, the exclusions in proposed subsections 16D(3)-(4), 16E(4)-(5), and 16F(6)-(7) would apply.³² Additionally, provision is made for the Attorney-General to determine that an entity is an exempt entity.³³ The Attorney-General's determination power to exempt an entity will be discussed later in this chapter.

2.20 The LCA suggested that it is unclear whether the exemption provisions would apply to sub-contractors:

It is not clear whether this exemption is intended to apply to sub-contractors of the entity which is the main contracted service provider. The Explanatory Memorandum states the intention of the exemption is to allow entities to engage in functions and activities such as information security tests. It would not be uncommon for such tests to be carried out by sub-contractors.³⁴

2.21 The AGD clarified that sub-contractors will be included in the exclusion that applies to contracted service providers as sub-contractors are included in the definition of 'contracted service provider' at section 6 of the Privacy Act.³⁵

Nature of offences and civil penalties

2.22 Some submitters were concerned that the offences were drafted too broadly. One submitter suggested that rather than considering whether re-identification was intentional, the offences should consider whether there was any intent to use the data to do harm.³⁶ Another submitter claimed that the 'intention' requirement within these offences is not clear.³⁷ The Australian Bankers' Association provided the following example of where it is not clear whether the intention requirement within the bill would be satisfied:

...a de-identified Government data set is used, and at some stage in the analytics process is combined with another data set, for commercial purposes including better consumer choice, and this leads to re-identification of the information.³⁸

31 Attorney-General's response, Senate Standing Committee for the Scrutiny of Bills, *Tenth report of 2016*, 30 Nov 2016 p. 668.

32 AGD, *Submission 6*, p. 6.

33 AGD, *Submission 6*, p. 6.

34 LCA, *Submission 10*, p. 10.

35 AGD, answers to questions on notice, 19 January 2017 (received 25 January 2017).

36 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 1.

37 Australian Bankers' Association Inc., *Submission 15*, p. 3.

38 Australian Bankers' Association Inc., *Submission 15*, p. 3.

2.23 While the AGD has not addressed this particular example, the AGD has clarified in its submission that:

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, 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.³⁹

2.24 A number of submitters noted that the Privacy Act only operates in Australia and therefore de-identification or disclosure which occurs outside of Australia would not be captured by the bill. For example, the OAIC noted that information now traverses national borders and regulatory jurisdictions and warned agencies to be mindful when releasing de-identified information as entities outside Australia may not be subject to the jurisdiction of the Privacy Act.⁴⁰

Breadth of the Minister's discretionary power to exempt

2.25 Proposed section 16G provides that the Minister may determine that an entity, or class of entities, is an exempt entity for the purposes of one or more of the offence provisions in relation to cryptology, information security, data analysis, or 'any other purpose that the Minister considers appropriate', and if the Minister is satisfied that it is in the public interest to do so. While the determination is a legislative instrument, it is not subject to disallowance pursuant to section 42 of the *Legislation Act 2003*.⁴¹

2.26 The Scrutiny of Bills Committee noted that the Minister's discretionary power to exempt an entity from proposed sections 16D, 16E or 16F is based on a single criterion: that the Minister is satisfied that it is in the public interest for the power to be exercised.⁴² The Scrutiny of Bills Committee indicated that this may suggest that the offence and civil penalty provisions are drawn too broadly.⁴³

39 AGD, *Submission 6*, p. 5.

40 OAIC, *Submission 5*, pp. 3–4.

41 Proposed subsection 16G(5).

42 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest 8 of 2016*, 9 November 2016, p. 34.

43 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest 8 of 2016*, 9 November 2016, p. 34.

2.27 In response to the concerns raised by the Scrutiny of Bills Committee, the Attorney-General advised that he considered the offence and penalty provisions of the bill appropriate and sufficiently defined. The Attorney-General explained that the exemption provision:

...is intended to provide an appropriate balance between protecting the privacy of individuals and allowing for legitimate research to continue...It is my expectation that the predominant reason for an exemption determination under section 16G will be in relation to the specific research purposes involving cryptology, information security and data analysis which is in the public interest. However, 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.

In view of the narrow scope of the proposed offences noted above, I do not expect there will be a large number of entities who will need exemptions for research in the public interest which requires the intentional re-identification of de-identified personal information published by a government agency.⁴⁴

2.28 In response to this assertion, the Scrutiny of Bills Committee reiterated its view that 'it is appropriate that Parliament define the boundaries of criminal wrong-doing rather than leaving these boundaries to depend (in part) on executive decision-making'.⁴⁵ While the Scrutiny of Bills Committee maintained its concerns, it noted the importance of the information provided by the Attorney-General as a point of access to understanding the law, and requested that key information be included in the EM.⁴⁶

2.29 Some submitters expressed concern about the Attorney-General's discretionary power to exempt certain entities.⁴⁷ The Australian Bankers' Association sought clarity on whether the Minister might exempt commercial organisations, such as banks, which it argues are also engaging in valuable research in areas of de-identification techniques, cryptology and information security.⁴⁸

2.30 The AGD provided further clarity about the process it would be undertaking to determine classes of exempt entities for the purpose of proposed section 16G:

44 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 668.

45 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 669.

46 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 669.

47 Australian Privacy Foundation, *Submission 11*, p. 3; Electronic Frontiers Australia, *Submission 14*, p. 3; and Australian Bankers' Association Inc., *Submission 15*, p. 4.

48 Australian Bankers' Association Inc., *Submission 15*, p. 4.

...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.⁴⁹

2.31 It was also raised that the Minister's determinations would not be subject to the rules of disallowance.⁵⁰ One submitter argued that preventing disallowance of potentially unfair decisions by the executive in relation to exemptions could lead to an erosion of the checks and balances that would normally be available.⁵¹

2.32 The EM explains why the rules of disallowance do not apply to the Minister's determinations. This includes providing commercial certainty to entities that would likely be undertaking projects or research activities which would involve a commercial benefit of some kind and would require a commitment of resources to undertake from the outset, as well as the time critical nature of some projects or research activities.⁵² Additionally, the requirement for the Minister to consult with the Commissioner prior to making any determination was considered to provide a degree of scrutiny and transparency.⁵³

2.33 The Scrutiny of Bills Committee considered that the rationale provided in the EM in relation to the Minister's determination not being subject to the rules of disallowance was sufficient, and made no further comment in relation to this issue.⁵⁴

Retrospectivity

2.34 A number of submitters raised concerns relating to the retrospective application of the bill.⁵⁵ If the bill is passed, the proposed new offences⁵⁶ would operate from 29 September 2016, being the date of the Attorney-General's media

49 AGD, *Submission 6*, p. 7.

50 Dr Peter Ansell, *Submission 3*, p. 4.

51 Dr Peter Ansell, *Submission 3*, p. 4.

52 EM, p. 27.

53 EM, p. 27.

54 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest 8 of 2016*, 9 November 2016, p. 36.

55 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 4; Mr Justin Warren, *Submission 2*, p. 4; Dr Peter Ansell, *Submission 3*, p. 3; LCA, *Submission 10*, pp. 8–9; Pirate Party Australia, *Submission 12*, pp. 3–4; and Australian Bankers' Association Inc., *Submission 15*, pp. 2–3.

56 Proposed ss 16D, 16E and 16F.

release advising of the government's intention to introduce a criminal offence of re-identifying de-identified government data.⁵⁷ It is noted that while proposed section 16F applies to conduct from 29 September which re-identifies personal information, the obligation to notify the responsible agency does not apply until after royal assent.

2.35 The LCA outlined its opposition to laws that apply retrospectively. In particular, it noted that retrospective measures generally offend rule of law principles, namely, that 'the law must be readily known and available, and certain and clear'.⁵⁸ It cited a number of High Court decisions which cautioned against retrospective legislation and emphasised the principle that the criminal law needs to be known by those who are subject to it.⁵⁹

2.36 The retrospective application of the bill was also raised by the Senate Standing Committee for the Scrutiny of Bills. The Scrutiny of Bills Committee noted that it has consistently commented on making 'legislation by press' and that its concerns are particularly acute in relation to provisions which create new offences.⁶⁰

2.37 In response to the Scrutiny of Bills Committee's concerns the Attorney-General acknowledged that while retrospective offences challenge a key element of the rule of law, the retrospective application of this bill was made clear when the amendments were announced. The Attorney-General explained that given the significant consequences for individuals if personal information was released, the government considered it important to provide a strong disincentive to entities who may have considered re-identification or disclosure of personal de-identified data while the Parliament considered the bill.⁶¹ The Scrutiny of Bills Committee acknowledged the importance of protecting privacy and reputation however, noting that:

...this is not, in itself, sufficient to override this general principle [that laws should only operate prospectively]. The importance of laws operating only prospectively is particularly acute in relation to the criminal law, where conduct should only be criminalised from the date the law making the conduct criminal commences. This supports long-recognised criminal law principles that there can be no crime or punishment without law.⁶²

57 Senator the Hon George Brandis QC, Attorney-General, 'Amendment to the Privacy Act to further protect de-identified data', *Media release*, 28 September 2016.

58 LCA, *Submission 10*, p. 9.

59 LCA, *Submission 10*, p. 9.

60 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest 8 of 2016*, 9 November 2016, p. 37.

61 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 671.

62 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 672.

2.38 The Parliamentary Joint Committee on Human Rights outlined its concerns relating to the incompatibility of these retrospective offences with article 15 of the *International Covenant on Civil and Political Rights* (ICCPR). The Human Rights Committee noted that 'as an absolute right that cannot be limited, there can be no justifiable limitation on the prohibition on retrospective criminal laws so as to accord with human rights law'.⁶³ It requested advice from the Attorney-General as to whether consideration has been given to amending proposed paragraphs 16D(1)(c) and 16E(1)(c) so that these sections operate from the date of Royal Assent. To date, the Attorney-General has not responded to the Human Rights Committee's report.

2.39 Several submitters referred to the ability of government to back-date laws to a press release date as setting a dangerous precedent.⁶⁴ While another submitter explained that after its first announcement, a spokesman for the Attorney-General's office informed the media that there would be provision made for legitimate research to continue. The submitter noted that they had interpreted this to mean that '*all*' legitimate research would be allowed as opposed to '*some*' legitimate research may be exempt.⁶⁵ The submitter stated that researchers may be left in the situation of being unable to tell the government what they had discovered during the time that they thought the investigation was legal.⁶⁶

2.40 The AGD explained that:

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.' The government considers that these narrowly prescribed offences meet these requirements.⁶⁷

2.41 The AGD went on to explain that the recently identified vulnerability in the Department of Health's dataset showed that there were gaps in privacy legislation and that the government acted immediately to strengthen protections for personal information against re-identification.⁶⁸ It noted that the bill provides a strong disincentive to entities who may have been tempted to attempt re-identification of any published datasets while the parliament considers the bill. Additionally, the AGD

63 Parliamentary Joint Committee on Human Rights, *Human rights scrutiny report: 9 of 2016*, 22 November 2016, p. 23.

64 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 4; Mr Justin Warren, *Submission 2*, p. 4; Dr Peter Ansell, *Submission 3*, p. 3; and Pirate Party Australia, *Submission 12*, p. 3.

65 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 4.

66 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 4.

67 AGD, *Submission 6*, p. 3.

68 AGD, *Submission 6*, p. 4.

explained that the government acted to ensure that the retrospective application is only for a short period of time.⁶⁹

Reverse burden of proof

2.42 Proposed subsections 16D(2)-(5), 16E(3)-(6) and 16F(5)-(8) of the bill provide a number of exemptions to the offences and civil penalties relating to re-identification and disclosure of de-identified personal information, and the requirement to inform the responsible agency of the de-identified information. In particular, these provisions reverse the burden of proof by requiring the entity to prove that the re-identification or disclosure of the de-identified information was consistent with one of the exemptions being:

- the entity is an agency and 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 the act under Australian law or court order;
- the entity was a contracted service provider for a Commonwealth contract to provide services for a responsible agency and the act was done for the purposes of meeting (directly or indirectly) an obligation under the contract;
- the entity 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; or
- the entity is an exempt entity for the purpose of a determination in force under section 16G and the act was done for a purpose specified in the determination and in compliance with any conditions specified in the determination.

2.43 The statement of compatibility contained in the EM noted that reversing the burden of proof is generally not consistent with the presumption of innocence under article 14(2) of the ICCPR, however it considered that in this case it was reasonable and appropriate for the burden of proof to be reversed.⁷⁰ The EM states that government does not anticipate that it will be difficult for an entity to demonstrate that its actions falls within one of the exemptions, that it is expected that the prosecution will not proceed where it is clear that the entity will rely on an applicable defence during the proceedings, and that it reflects the seriousness of the prohibited conduct.⁷¹

2.44 The Parliamentary Joint Committee on Human Rights considered the information provided within the EM and concluded the reversed burden of proof contained within the bill was compatible with the presumption of innocence contained in article 14 of the ICCPR on the basis that the burden was evidentiary in nature,

69 AGD, *Submission 6*, p. 4.

70 EM, p. 8.

71 EM, p. 8.

rather than legal.⁷² The Human Rights Committee expressed the view that 'the measures are likely to be a proportionate limitation on the presumption of innocence'.⁷³

2.45 The Scrutiny of Bills Committee also considered the information contained within the EM and sought further justification from the Attorney-General and requested that the principles set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide) be addressed.⁷⁴ In response to concerns raised by the Scrutiny of Bills Committee the Attorney-General explained that relevant matters would be peculiarly within the knowledge of the defendant and it would be significantly more difficult and costly for the prosecution to prove that the exclusion did not apply.⁷⁵

2.46 However, the Scrutiny of Bills Committee noted that page 50 of the Guide states that the fact that it is difficult for the prosecution to prove a particular matter has not traditionally been considered a sound justification for placing a burden of proof on the defendant.⁷⁶ Despite the additional information provided by the Attorney-General, the Scrutiny of Bills Committee remained of the view that the reversal of the evidentiary burden of proof may not be framed in accordance with the relevant principles set out in the Guide:

...it is not apparent to the committee that it would be particularly onerous for the prosecution to prove the existence of an agreement or contract with the Commonwealth, given there does not seem to be any impediment on the Commonwealth supplying evidence of that agreement or contract to the prosecution. It is also not apparent, on the information provided to the committee, that such matters would be *peculiarly* within the knowledge of the defendant.⁷⁷

72 Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny: 9 of 2016*, 22 November 2016, pp. 25-26.

73 Parliamentary Joint Committee on Human Rights, *Human Rights Scrutiny: 9 of 2016*, 22 November 2016, p. 26.

74 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest 8 of 2016*, 9 November 2016, p. 33.

75 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 666.

76 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 666.

77 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 666.

2.47 The Scrutiny of Bills Committee noted the importance of the information provided by the Attorney-General as a point of access to understanding the law, and requested that the information be included in the EM.⁷⁸

Committee View

2.48 The committee notes the concerns that have been expressed about aspects of this bill by submitters, including the introduction of criminal offences, the reversed burden of proof and the retrospective application of the bill. However, given the gap that was recently identified in privacy legislation, the committee is of the view that the bill provides a necessary and proportionate response. In arriving at this conclusion the committee has given careful consideration to the need to balance the benefits that open data can provide with the need to strengthen the protections to the privacy of Australians while also continuing to encourage research in the areas of information security. The committee considers that the bill achieves this outcome.

2.49 The committee acknowledges the Scrutiny of Bills Committee's comments on retrospective legislation—and the information provided by the Attorney-General and published in that committee's Tenth Report of 2016—and is generally reluctant to endorse laws that operate retrospectively. However, in this instance the committee notes that the Minister's announcement was in the current term of parliament, was very specific, and indicated clearly that the legislation was to apply from the date of the announcement. There is sufficient particularity in the announcement to alert would-be offenders of the nature of the offence.

2.50 The committee also notes concerns expressed by the research community but has formed the view that researchers employed by States and Territories (which includes most universities) will not fall within the scope of the Privacy Act. Additionally, the bill has exclusions for agencies in connection with their functions and activities or authorised by law, for contracted service providers for the purpose of meeting an obligation under a Commonwealth contract and for entities in accordance with an agreement between the entity and the responsible agency. Moreover, the committee is reassured by the consultation process the AGD will put in place to ensure that researchers not connected to universities will have an opportunity to be considered within a class of entities subject to the Minister's exemption determination powers.

78 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 666.

Recommendation 1

2.51 The committee recommends that the bill be passed.

**Senator the Hon Ian Macdonald
Chair**

Dissenting Report of the Australian Labor Party and Australian Greens

1.1 Labor and Greens Senators are of the view that the Privacy Amendment (Re-identification Offence) Bill 2016 (the bill) should not be passed as it provides a disproportionate response to the identified gap in the *Privacy Act 1988* (Privacy Act) and the bill does not achieve its objectives.

1.2 The privacy of Australians is of paramount importance; however, a careful balance must be achieved between maintaining privacy, ensuring that government agencies properly de-identify datasets prior to its publication, and encouraging research into the areas of information security, cryptology and data analysis. The bill fails to provide a holistic response and neglects to consider the de-identification process and consequences for agencies for releasing datasets that have been poorly de-identified. As outlined by the NSW Office of the Privacy Commissioner:

...it places a disproportionately high onus on external recipients to be aware which released datasets are considered to have undergone a de-identification process. The proposed provisions do not appear to create corresponding obligations on the releasing entities to certify each released dataset as deriving from personal data or the treatment used to achieve the outcome of non-identifiable data.¹

1.3 Rather, if passed, the bill adopts a punitive approach towards information security researchers and research conducted in the public interest. In contrast, government agencies that publish poorly de-identified information do not face criminal offences and are not held responsible. While the Privacy Act does not apply to most Australian universities, as outlined by Melbourne university researchers, the implications of the bill are not clear for researchers at the Australian National University, students, and individuals acting on their own initiative who happen to be university employees.² Additionally, no consideration has been given as to whether an individual who re-identifies their own information, or their dependent's or client's information, should also be subject to the bill.³ The bill discourages research conducted in the public interest as well as open discussion of issues which may have been identified.

1.4 Labor and Greens Senators are opposed to the retrospective application of the bill and agree with the concerns raised by the Senate Scrutiny of Bills Committee and the Law Council of Australia that retrospective provisions offend a fundamental principle in the rule of law and that this is particularly acute in the case of criminal offences.⁴

1 NSW Office of the Privacy Commissioner, *Submission 13*, p. 2.

2 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 3.

3 Dr Peter Ansell, *Submission 3*, p. 2.

4 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 672; and Law Council of Australia, *Submission 10*, p. 9.

1.5 Moreover, while the Attorney-General has claimed that the retrospective application of this bill was made clear in his announcement on 28 September 2016, the submission by the Melbourne university researchers indicates a level of ambiguity. They explain that they had interpreted a commitment that 'all legitimate research would be allowed to continue [as opposed to] some designated research should be exempt'.⁵

1.6 Labor and Greens Senators also disagree with reversing the evidential burden of proof. As justification for reversing the burden of proof, the Explanatory Memorandum noted that it would not be difficult for the entity to demonstrate that one of the exemptions apply and that it also reflects the seriousness of the prohibited conduct.⁶ However, as outlined by the Senate Scrutiny of Bills Committee, the fact that it would be easy for an entity to provide evidence that one of the exemptions apply, or conversely, that it may be difficult for the prosecution to prove that the exemption does not apply, is not sufficient justification for reversing the burden of proof.⁷ Also, it is not apparent that it would be particularly onerous for the prosecution to prove that the exemption did not apply.⁸ As such, the justification for reversing the burden of proof is neither reasonable nor appropriate.

Conclusion

1.7 The bill provides a disproportionate reaction to the identified gap in the Privacy Act. It neglects the initial process of de-identification and does not hold government agencies responsible for publishing poorly de-identified datasets. Instead it penalises public interest research and discourages open investigation and discussion of potential issues relating to information security. The disproportionate response is also evidenced through the retrospective application of the bill as well as the reversal of the burden of proof.

Recommendation 1

1.8 Labor and Greens Senators recommend that this bill not be passed.

Senator Louise Pratt
Deputy Chair

Senator Nick McKim

5 Mr Christopher Culnane, Mr Benjamin Rubinstein and Dr Vanessa Teague, *Submission 1*, p. 4.

6 Privacy Amendment (Re-identification Offence) Bill 2016, Explanatory Memorandum (EM), p. 8.

7 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 666.

8 Senate Standing Committee for the Scrutiny of Bills, *Tenth Report of 2016*, 30 November 2016, p. 666.

Appendix 1

Public submissions

- 1 Chris Culnane, Benjamin Rubinstein, Vanessa Teague
- 2 Mr Justin Warren
- 3 Dr Peter Ansell
- 4 Ms Rosie Williams
- 5 Office of the Australian Information Commissioner
- 6 Attorney-General's Department
- 7 Mr Andrew van der Stock
- 8 DIGI
- 9 Mercury Information Security Services
- 10 Law Council of Australia
- 11 Australian Privacy Foundation
- 12 Pirate Party Australia
- 13 Office of the Privacy Commissioner NSW
- 14 Electronic Frontiers Australia
- 15 Australian Bankers' Association Inc.

Answers to questions on notice

- 1 Attorney-General's Department – answers to questions taken on notice, 19 January 2017 (received 25 January 2017).

