Australian Government
Office of the Australian Information Commissioner

Review of the mandatory data retention regime

Submission of the Office of the Australian Information Commissioner

oaic.gov.au

OAIC

Contents

Submission to the review of the mandatory data retention regime

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee's) Review of the mandatory data retention regime (the Regime).

2. The OAIC is an independent Commonwealth statutory agency established to bring together the functions of oversight of privacy protection, freedom of information and information policy. The *Privacy Act 1988* (Cth) (Privacy Act) confers on the Australian Information Commissioner and Privacy Commissioner a range of privacy regulatory functions and powers. In performing these functions, the Commissioner is required to have regard to the objects of the Privacy Act.[1] The objects include promoting the protection of the privacy of individuals, implementing Australia's international obligations in relation to privacy, promoting responsible and transparent handling of personal information as well as recognising that the protection of the privacy of individuals must be balanced with the interests of entities in carrying out their functions and activities.[2]

3. Where law enforcement initiatives adversely impact privacy, they must be subject to a careful and critical assessment of their necessity, reasonableness and proportionality.[3] This includes demonstrating the necessity of the initiative through empirical evidence, where available, and ensuring that the scope of proposed measures is as clear and transparent as possible and subject to appropriate safeguards.

4. Telecommunications data[4] can form a detailed picture of an individual's habits and identity.[5] The richness of this information, when considered alongside the scale of telecommunications data collected as part of the Regime increases the risk to an individual's privacy commensurate with the nature and quantity of the personal information held.

5. The OAIC has previously provided a submission on the Inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*.[6] In that submission, the OAIC made 18 recommendations to assist the Committee in determining whether the Regime appropriately balances the needs of Australian enforcement and security agencies to access telecommunications data with the protection of the privacy of individuals. That submission focused on the adequacy of privacy safeguards established in legislation to ensure that the laws

---

[1] Section 29 of the Privacy Act.

[2] Section 2A of the Privacy Act.

[3] As raised in our previous submission, the Office of the United Nations High Commissioner for Human Rights has stated in relation to privacy that '[A] limitation must be necessary for reaching a legitimate aim, as well as in proportion to the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal.' See Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014), p23.

[4] Under the Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act), service providers must collect and store certain kinds of information about individuals' communications (hereinafter referred to as 'telecommunications data').

[5] This was acknowledged in our previous submission in paragraph 8 and 18. Refer to: https://www.oaic.gov.au/engage-with-us/submissions/submission-on-the-inquiry-into-the-telecommunications-interception-and-access-amendment-data-retention-bill-2014.

[6] See <https://www.oaic.gov.au/engage-with-us/submissions/submission-on-the-inquiry-into-the-telecommunications-interception-and-access-amendment-data-retention-bill-2014>.

were reasonably necessary and proportionate to achieving a legitimate purpose, particularly given the application of the Regime to all individuals.

6. Some of the issues raised in the OAIC's previous submission were addressed in the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (amending Act). However, other key recommendations that sought to establish privacy safeguards to ensure the proportionality of the Regime were not adopted or fully adopted. Those earlier recommendations include:

    - that the Regime only require service providers to retain telecommunication information for the minimum amount of time necessary to meet law enforcement needs[7]

    - that clear and narrowly defined language be used in the Regime, particularly to describe the kinds of information that service providers are required to collect and store under the Regime to effectively implement the intentions of the scheme and reduce uncertainty for service providers that collect and retain data[8]

    - that in the absence of a warrant-based access scheme, the need to limit the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to prevent or detect a serious offence and safeguard national security,[9] and

    - recognising the important safeguards in limiting access to agencies involved in the detection of a serious offence and safeguarding national security, that any expansion of the definition of 'enforcement agency' be made by amendment to the TIA Act itself.[10]

7. This review comes at a time when domestic and international developments have heightened the community's concern for the protection of their personal information. Information available about the operation of the Regime to date indicates that a range of agencies are accessing telecommunications data, outside the legislative framework that established the Regime.[11] Also, the Regime does not limit access to telecommunications data for the purposes of investigating serious criminal offences or in relation to national security. Further, information from the operation of the Regime to date indicates that the majority of telecommunications data accessed is less than 12 months old.[12] Internationally, there has been further jurisprudence

---

[7] Refer to paragraph 35-44 of our previous submission. In the earlier submission, the OAIC stated (at paragraph 44): I recommend that the Statement clearly set out evidence that shows why it is necessary to retain telecommunications data for a minimum of two years (or, in the case of certain subscriber information, for longer periods). If that is not practicable because of confidentiality or security reasons, then it may be open to the Committee to request and consider the evidence that establishes the necessity of the retention of each of the kinds of data proposed to be collected and retained, and the length of the retention period for each kind of data.

[8] This includes ensuring terms of the Act are sufficiently clear and narrowly defined to effectively implement the specific intentions of the Regime. Refer to paragraph 26-34 of our previous submission.

[9] Refer to paragraph 63-75 of our previous submission.

[10] Refer to paragraph 76-80 of our previous submission.

[11] The Commonwealth Ombudsman's submission to the Committee at p.7 notes that during their inspections, it was revealed that 'some agencies have sought access to telecommunications data under the following legislation: Telecommunications Act 1997, Migration Act 1958, and Coroners Act 1995 (Tas)'.

[12] From 2017-18, 242,843 authorised disclosures were for telecommunications data aged 0-12 months old, the total amount of disclosures being 263,462.See the Annual report of 2017-18 for more: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance.

since 2015 that has found similar schemes to the Australian Regime to unnecessarily intrude upon privacy. In light of these developments, the OAIC considers that it is appropriate for further privacy safeguards to be incorporated into the Regime.

8. Accordingly, the OAIC recommends that the Committee:

    - seek to define the terms 'content' and 'substance' of a communication[13] to reduce the potential for more personal information to be collected than is necessary for the purposes of the Regime[14]
    - consider reducing the retention period to better ensure the proportionality of the Regime
    - amend the TIA Act to incorporate an express obligation on service providers and enforcement bodies to destroy or de-identify telecommunications data after a specifically defined period
    - implement measures to restrict the agencies that are permitted to access telecommunications data so that agencies able to access telecommunications data are limited to those covered by safeguards in the TIA Act
    - require that any increases to the scope of the agencies permitted to access telecommunications data under the Regime be made through legislative amendment to the TIA Act rather than legislative instrument to ensure transparency and accountability, and that s 176(5) be amended to include a requirement for the Information Commissioner to be consulted before additional authorities or bodies are declared to be 'enforcement agencies' or the categories of retained metadata are increased
    - consider introducing a warrant-based scheme to access telecommunications data
    - reconsider limiting the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to investigate a serious offence and safeguard national security.

The OAIC's regulatory role

9. The Privacy Act contains 13 Australian Privacy Principles (APPs) which set out obligations regarding the handling of personal information by regulated entities and rights for individuals. A central principle in the Privacy Act is the requirement that regulated entities must take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure.[15] This Committee has previously

[13] Section 172 of the TIA Act does not allow the disclosure to an agency of information that is the content or substance of a communication, or a document that contains the content or substance of a communication. The term 'content or substance of a communication' is not defined in the TIA Act.

[14] The Commonwealth Ombudsman's submission to the Committee at p.6 offers some guidance in that the majority of telecommunications data the Ombudsman inspects, it is able to determine whether the disclosed information breaches the restriction in s 172. For example, the telecommunications data of a phone call can include the date, time and location(s) of the call but cannot include the substance of what the parties said.

[15] APP 11, Schedule 1 of the *Privacy Act*.

recommended that a mandatory data retention regime should be underpinned by a mandatory data breach notification scheme'.[16]

10. Since February 2018, entities must notify affected individuals and the OAIC in the event of a serious data breach.[17] These are important obligations which safeguard the security of individuals' personal information and increase the accountability of regulated entities where personal information is breached.

11. Under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), service providers must collect and store certain kinds of information about individuals' communications.[18] Section 187LA of the TIA Act deems this telecommunications data to be personal information for the purposes of the Privacy Act. Accordingly, all entities that collect, use and disclose telecommunications data are regulated by the OAIC, to the extent that the entities' activities relate to telecommunications data.[19]

12. Provisions of the *Telecommunications Act 1997* (Telecommunications Act) and the TIA Act allows for the disclosure of certain information by service providers to enforcement agencies in certain circumstances. If service providers disclose information under certain provisions of the Telecommunications Act or the TIA Act, they must create and keep a record of the disclosure.[20] Part 13 Division 5 of the Telecommunications Act authorises the OAIC to monitor compliance by service providers with those record keeping requirements. Provisions of the TIA Act expressly confer powers of oversight on the Commonwealth Ombudsman over enforcement agencies' access to telecommunications data under the TIA Act.[21]

13. The acts and practices of intelligence agencies are not subject to the Privacy Act.[22] Enforcement bodies, as defined in s 6 of the Privacy Act, are broadly subject to the Privacy Act, however there are limitations to the extent to which the APPs in the Privacy Act apply to the operations of these bodies. For example, the limitation on using or disclosing information collected for a particular purpose other than the primary purpose does not apply where authorised by law or where the entity reasonably believes it necessary for an enforcement related activity.[23]

---

[16] PJCIS, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, p. 192.

[17] Part IIIC of the *Privacy Act*. Entities with security obligations under the Privacy Act are required to notify individuals and the OAIC of an 'eligible' data breach. A data breach is 'eligible' if it is likely to result in serious harm to any of the individuals to whom the information relates. More information on eligible data breaches is available on the OAIC's website at <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches>.

[18] These are outlined in s 187AA of the TIA Act.

[19] Section 187LA of the TIA Act.

[20] The records of disclosures made under the TIA Act must comply with the specific requirements contained in ss 306 and 306A of the Telecommunications Act.

[21] The Commonwealth Ombudsman does not have oversight in relation to access to telecommunications data under legislation other than the TIA Act. For further information see pp. 7-8 of the Commonwealth Ombudsman's submission to the Committee available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime/Submissions.

[22] Section 7 of the Privacy Act details the specific authorities and bodies whose acts and practices are exempt from the Privacy Act. This includes intelligence agencies under ss 7(1)(f), defence intelligence agencies under s 7(1)(a) and specific law-enforcement agencies, under ss 7(1)(ga) and (h).

[23] APP 3 (collection of solicited personal information) and APP 6 (use or disclosure of personal information) listed in Schedule 1 of the Privacy Act provide exceptions to certain law-enforcement entities regulated under the Privacy Act

14. The OAIC has undertaken a range of activities to assist and monitor entities with responsibilities under the Regime. Prior to the commencement of the Regime, the OAIC issued guidance for entities on their Privacy Act obligations.[24] This was supplemented by a Privacy Act compliance self-assessment tool and engagement with small telecommunications service providers.[25] The OAIC also engaged with large telecommunications service providers during the Regime's implementation period to understand industry's approach to implementing the new TIA Act requirements.

15. Prior to the commencement of the Regime, the OAIC conducted a series of assessments of telecommunications service providers in relation to any privacy risks arising in their processes and associated systems for disclosing personal information to law enforcement agencies under the TIA Act.[26] The OAIC has ongoing assessments of how telecommunications service providers secure the telecommunications data that they collect and hold under the Regime.

16. The OAIC has also conducted assessments of service providers' record keeping obligations when disclosing personal information to law enforcement under the Telecommunications Act.[27]

Appropriateness of the dataset and retention period

The contents and substance of a communication

17. Section 187AA of the TIA Act sets out the kinds of information a service provider is required to keep under the Regime. This provision is read in conjunction with s 187A of the TIA Act, which notes that service providers are not required to keep 'information that is the contents or substance of a communication'. The terms 'contents' and 'substance' are not defined in the TIA Act.

18. The OAIC considers that clarifying these terms would create greater certainty and enhance privacy protections by reducing the potential for more personal information to be collected than is necessary for the purposes of the Regime. With this in mind, the OAIC recommends that the Committee consider amending the TIA Act to define the terms 'contents' and 'substance' where they appear.

---

from meeting APP 3 and APP 6 obligations that would otherwise apply, under s 3.4(a) and (d), and s 6.2(b) and (e) respectively.

[24] Refer to https://www.oaic.gov.au/privacy/guidance-and-advice/telecommunications-service-providers-obligations-arising-under-the-privacy-act-1988-as-a-result-of-part-5-1a-of-the-telecommunications-interception-and-access-act-1979/.

[25] Refer to https://www.oaic.gov.au/privacy/guidance-and-advice/self-assessment-checklist-privacy-obligations-under-the-data-retention-scheme/.

[26] Refer to https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-oaic-assessment-of-telecommunication-organisations-information-security-practices-when-disclosing-personal-information-under-the-telecommunications-interception-and-access-act-1979/.

[27] Refer to https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-follow-up-of-s309-telecommunication-inspections/ and https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-follow-up-of-s309-telecommunication-inspections/.

Recommendation 1

The OAIC recommends that the TIA Act be amended to clearly seek to define the terms 'content' and 'substance' of a communication to reduce the potential for more personal information to be collected than is necessary for the purposes of the Regime.

The two-year retention period

19. The Explanatory Memorandum to the amending Act states that 'a retention requirement is consistent with the aim of the legislation and is necessary having regard to the reasonable requirements of national security and enforcement agencies to have telecommunications data available for investigations.'[28] As the OAIC raised in its 2015 submission to the Committee, evidence should be provided to the public to demonstrate the proportionality of this measure.

20. Statistics on the operation of the Regime indicate that the majority of data requested by law enforcement agencies is less than three months old. Statistics from the periods 2015-16 and 2016-17 demonstrate that of all authorised disclosures of telecommunications data by service providers, approximately:

- 83% of disclosed data was 0-3 months old[29], 94% of disclosed data was 0-12 months old,[30] and less than 2% of disclosed data was over 24 months old[31] for the 2015-16 year, and
- 79% of disclosed data was 0-3 months old[32], 93% of disclosed data was 0-12 months old,[33] and less than 1% of disclosed data was over 24 months old[34] for the 2016-17 year.

21. While the OAIC appreciates that a reduction in the data retention period may impact on some law enforcement activities, the statistics reported from enforcement agencies suggest that the continued retention of data for two years may not be proportionate to the privacy impacts on individuals. Given that a majority of authorisations made were for data less than 12 months old,

[28] *Explanatory Memorandum*, p. 48.

[29] From 2015-16, 196,646 authorised disclosures were for telecommunications data aged 0-3 months old, the total amount of disclosures being 237,071. See the Annual Report of 2015-16 for more: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance.

[30] From 2015-16, 225,169 authorised disclosures were for telecommunications data aged 0-12 months old, the total amount of disclosures being 237,071.

[31] From 2015-16, 4,499 authorised disclosures were for telecommunications data aged over 24 months, the total amount of disclosures being 237,071.

[32] From 2016-17, 230,176 authorised disclosures were for telecommunications data aged 0-3 months old, the total amount of disclosures being 292,463. See the Annual report of 2016-17 for more: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance.

[33] From 2016-17, 274,481 authorised disclosures were for telecommunications data aged 0-12 months old, the total amount of disclosures being 292,463.

[34] From 2016-17, 4,536 authorised disclosures were for telecommunications data aged over 24 months, the total amount of disclosures being 292,463.

the OAIC recommends that the Committee consider a reduction of the two-year retention period.

Recommendation 2

The OAIC recommends that the Committee consider reducing the retention period to better ensure the proportionality of the Regime.

Security requirements in relation to data stored under the Regime

22. In its previous submission, the OAIC recommended that the Regime only require service providers to retain the minimum amount of information for the minimum amount of time necessary. The requirement to destroy or de-identify personal information is an obligation that applies to all entities that collect and use telecommunications data under the Regime (aside from intelligence agencies) under APP 11.2.

23. Under the Regime, this requirement will not be enlivened in relation to telecommunications data collected by service providers for at least two years after the time the data was collected. Under s 187C(3) of the TIA Act, the requirement to retain telecommunications data for two years does not prevent a service provider from keeping that data for a longer period, provided that they are legally authorised to do so. There is similarly no defined timeframe under the Regime for the destruction of telecommunications data obtained by an enforcement body.

24. The potential consequences of data and security breaches increase with the quantities of personal information retained. The OAIC considers that privacy protection of individuals would be improved if the Regime were to incorporate an express obligation on both service providers and enforcement bodies to destroy or de-identify telecommunications data after a specifically defined period.

Recommendation 3

The OAIC recommends amending the TIA Act to incorporate an express obligation on service providers and enforcement bodies to destroy or de-identify telecommunications data after a specifically defined period.

Access by agencies to retained telecommunications data

25. In its Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, the Committee recommended that enforcement agencies, which are agencies authorised to access telecommunications data under internal authorisation, be

specifically listed in the TIA Act.[35] The Committee made this recommendation in recognition that

> 'the degree of intrusion into privacy resulting from access to telecommunications data will depend significantly on the type and amount of telecommunications data accessed. The Committee considers that in the context of the modern telecommunications environment, and in particular the proposed data retention regime, there is potential for access to telecommunications data to amount to a very significant intrusion into privacy by an agency…For this reason, consistent with proposed measures to safeguard access to stored communications, the Committee considers that those agencies able to access telecommunications data should be listed in the legislation'.[36]

26. The TIA Act was amended to specify the agencies that were permitted to have access to telecommunications data. This was a measure that sought to mitigate privacy risks to individuals.

27. The OAIC is aware of reported instances of certain bodies not permitted to access telecommunications data under the TIA Act, including federal, state and local agencies, requesting access to data under provisions of the Telecommunications Act.[37] This matter has been raised previously during the Committee's hearings on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018.[38] We understand that generally, these bodies have relied on alternate legislative provisions, namely, ss 280(1)(b) and s 313 of the Telecommunications Act, which:

- allow the 'disclosure or use of information of a document if… the disclosure or use is required or authorised by or under law', thereby allowing agencies to use their own powers to seek access to such data, and
- require carriers, 'carriage service providers' and carriage service intermediaries to 'give officers and authorities of the Commonwealth and of the States and Territories such help as is reasonably necessary' for law enforcement purposes.

28. The OAIC recommends that the Committee consider implementing an enforceable restriction on the agencies that are permitted to access telecommunications data, noting this was a safeguard that provided privacy protections in the absence of more formal mechanisms such as a warrant-based access regime. As the law currently stands, there appears to be mechanisms for accessing telecommunications data outside of the TIA Act that, while permitted, have the practical impact of reducing the effectiveness of safeguards in the TIA Act.

---

[35] Refer to Recommendation 21, p. 215.

[36] Refer to paragraphs 6.88-6.91 of the Committee's Advisory Report.

[37] The Commonwealth Ombudsman's submission to the Committee at p.7 which revealed that some agencies have sought access to telecommunications data outside of the TIA Act.

[38] During the Committee's hearing on the *Telecommunications (Interception and Access) Bill 2018* on 19 October 2018, representatives from the Communications Alliance brought to the attention of the Committee the fact that requests for metadata are being made outside of the Regime established in the TIA Act. Requests to Communications Alliance members are estimated to average approximately 350,000 a year. See pages 41-42 of the Hansard transcript, available online: <https://parlinfo.aph.gov.au/parlInfo/download/committees/commjnt/2a1771c8-f314-43f2-b9b0-cd09ad8123ae/toc_pdf/Parliamentary%20Joint%20Committee%20on%20Intelligence%20and%20Security_2018_10_19_6680_Official.pdf;fileType=application%2Fpdf#search=%222010s%20parliamentary%20joint%20committee%20on%20intelligence%20and%20security%22>.

Recommendation 4

The OAIC recommends that the Committee implement measures to restrict the agencies that are permitted to access telecommunications data so that agencies able to access telecommunications data are limited to those covered by safeguards in the TIA Act.

29. Under the TIA Act, the Minister may declare an authority or body to be an enforcement agency for the purpose of the Regime by legislative instrument, rather than by an amendment to the TIA Act.[39] The Minister may also declare, by legislative instrument, that certain kinds of personal information be retained by service providers for the purpose of the Regime. It is at the discretion of the Minister to consult with the Privacy Commissioner and the Ombudsman on these matters.[40]
30. While the OAIC notes that s 176A of the TIA Act provides some mechanisms to ensure that any permanent expansion to the group of enforcement agencies is done by way of an amendment to the TIA Act, there remains the potential for an expansion of the Regime with limited parliamentary scrutiny, public debate or oversight. Considering the large amounts of personal information already retained as part of the Regime, the OAIC recommends that any increases to the scope of the Regime are made through legislative amendment to the TIA Act to promote transparency for the public and ensure accountability.
31. The OAIC also recommends that s 176(5) be amended to include a requirement for the Information Commissioner to be consulted before additional authorities or bodies are declared to be 'enforcement agencies' or the categories of retained metadata are increased.

Recommendation 5

The OAIC recommends that any increases to the scope of agencies permitted to access telecommunications data under the Regime be made through legislative amendment to the TIA Act rather than legislative instrument to ensure transparency and accountability, and that s 176(5) be amended to include a requirement for the Information Commissioner to be consulted before additional authorities or bodies are declared to be 'enforcement agencies' or the categories of retained metadata are increased.

Purpose and authorisation for accessing telecommunications data

32. In its 2015 submission, the OAIC recommended that the use and disclosure of telecommunications data under the Regime should only occur where it is reasonably necessary to prevent or detect a serious offence and safeguard national security, in order to mitigate the privacy impact of the Regime.[41]

[39] Section 176A(3) of the TIA Act.
[40] Section 176A(5) of the TIA Act.
[41] Refer to paragraph 70-75 of our previous submission.

33. This threshold was not adopted and the offences for which telecommunications data can be accessed under the TIA Act are not specified.[42]

34. There is heightened community awareness and concern about privacy and the security of personal information.[43] There have also been developments in comparable jurisdictions (discussed later in this submission) that emphasises the role of strong procedural safeguards in relation to accessing telecommunications data. Recognising that technological developments will continue to increase the particularity of telecommunications data and the information it reveals about individuals, it is appropriate that strong procedural safeguard to mitigate the privacy impacts of telecommunications data are added to the Regime.

35. Accordingly, the OAIC recommends that the Committee consider introducing a warrant-based scheme to access telecommunications data as the primary mechanism through which the privacy intrusive nature of the Regime is proportionately balanced against legitimate law enforcement objectives.

36. The OAIC also asks the Committee to reconsider limiting the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to investigate a serious offence and safeguard national security. This would adopt the threshold for access that is applied for access to prospective telecommunications data under s 180 of the TIA Act.

Recommendation 6

The OAIC recommends that the Committee consider introducing a warrant-based scheme to access telecommunications data.

Recommendation 7

The OAIC recommends that the Committee reconsider limiting the purpose for which an authorisation to disclose telecommunications data can be made to where it is reasonably necessary to investigate a serious offence and safeguard national security.

Developments in international jurisdictions since the passage of the Bill

37. The *International Covenant on Civil and Political Rights* (ICCPR) provides for the protection of individuals from arbitrary or unlawful interference with their privacy, family home or

[42] The TIA Act Annual Report 2016-17 prepared by the Department of Home Affairs notes that while telecommunications data is accessed in the investigation of offences such as homicide and terrorism offences, telecommunications data is also accessed for what appears to be less serious offences such as offences relating to traffic and unlawful entry.

[43] The 2017 Australian Community Attitudes to Privacy Survey results indicated that the majority of Australians are concerned about online privacy, with 69% of Australian more concerned about online privacy than five years prior.

correspondence,[44] and this protection is reflected in article 17 of the ICCPR. While Australia's privacy laws recognise that the protection of individuals' privacy is not an absolute right, any instance of interference must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality.

38. Since the implementation of the Regime, there have been significant developments in international law concerning telecommunications data retention schemes.

39. For context, the European Union (EU's) Data Retention Directive was passed in 2006 and required that telecommunications providers retain traffic and location data belonging to individuals or legal entities. The retention period was to be between six months and two years, and the Directive's purpose was to assist member states in preventing, investigating, detecting and prosecuting serious crime, such as organised crime and terrorism.[45]

40. The Directive was challenged on the grounds of an infringement to the right to private life, and the right to the protection of personal data of individuals, as reflected in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU).[46]

41. In a ruling of 8 April 2014, in the *Digital Rights Ireland* case,[47] the Court of Justice of European Union (CJEU) annulled the Directive on the basis that it 'entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary'.[48]

42. Notably, as was recognised by the Committee, the Bill that ultimately established the Regime was based on the EU's Directive.[49]

43. Subsequently, there have been several legal challenges to legislation that sought to introduce data retention schemes but have been ruled invalid due to their inconsistency with Articles 7 and 8 of the CFREU.

44. In the United Kingdom, after the *Data Retention and Investigatory Powers Act 2014* was ruled invalid on the basis that it was inconsistent with EU law, the Government enacted the *Investigatory Powers Act 2016* (UK) (IPA). Consistent with the ruling established in the *Digital Rights Ireland* case, the High Court in the United Kingdom ruled in April 2018 that certain provisions of the new IPA were invalid on the basis that they were not proportionate to the

---

[44] *International Covenant on Civil and Political Rights,* opened for signature on 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

[45] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, Article 6 and 1, paragraph 1. See: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[46] Charter of the Fundamental Rights of the European Union, 2012 O.J. (C 326), pg. 391. See: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

[47] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregoering ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014). See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293.

[48] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregoering ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014), paragraph 65. See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293.

[49] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Bill 2014,* p. 61.

privacy intrusions that they would necessarily involve. Specifically, authorisations for access to data could not be issued without independent judicial oversight or authorisations, and for reasons that were not relevant to the investigation of serious crime.[50] Amendments to the IPA in recognition of the High Court ruling have added procedural safeguards to the collection of telecommunications data and narrowed the breadth of offences for which telecommunications data can be collected.[51]

45. The laws of other countries that have enacted a telecommunications data retention regime are not binding on Australia, but nonetheless indicate how other jurisdictions have sought to balance the proportionality of law enforcement objectives and human rights obligations.

46. Compared to other data retention regimes in overseas jurisdictions, as listed in the Department of Home Affairs submission to this review,[52] Australia is one of a small proportion of jurisdictions that have a data retention period of two years or longer. Most jurisdictions have a one-year retention period, including the United Kingdom. Amongst the same cohort, around half of the jurisdictions are noted as having their data retention regime declared invalid or subject to challenge.[53]

47. Developments in comparable jurisdictions since the introduction of the Regime add further weight to the need to consider the additional privacy safeguards outlined in this submission.

48. The OAIC is available to provide further information or assistance to the Committee as required.

Angelene Falk
Australian Information Commissioner
Privacy Commissioner

[50] *R (National Council for Civil Liberties (Liberty)) v Secretary of State for the Home Department, Secretary of State for Foreign and Commonwealth Affairs* [2018] EWHC 975.

[51] Refer to the *Data Retention and Acquisition Regulations 2018* (UK).

[52] Refer to pp 40-43.

[53] See Home Affairs submission to the Committee at Appendix A.