Australian Human Rights Commission

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

AUSTRALIAN HUMAN RIGHTS COMMISSION SUBMISSION TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

14 January 2015

ABN 47 996 232 602
Level 3, 175 Pitt Street, Sydney NSW 2000
GPO Box 5218, Sydney NSW 2001
General enquiries 1300 369 711
Complaints info line 1300 656 419
TTY 1800 620 241

Australian Human Rights Commission
www.humanrights.gov.au

Table of Contents

1 Introduction

1. The Australian Human Rights Commission makes this submission to the Parliamentary Joint Committee on Security and Intelligence in its Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill).

2. The Commission is established by the *Australian Human Rights Commission Act 1986* (Cth) and is Australia's national human rights institution.

3. This submission addresses the potential impact of the Bill on human rights and in particular the rights to privacy and freedom of expression. These rights, reflected in articles 17 and 19 of the *International Covenant on Civil and Political Rights* (ICCPR),[1] may be limited by proportionate measures to achieve a legitimate aim, if protected by safeguards and oversight.

2 Summary

4. The Bill amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to introduce a mandatory data retention scheme. This scheme would require service providers to retain certain types of telecommunications data to be prescribed by Regulation for two years. The data would then be available for police, the Australian Security Intelligence Organisation (ASIO) and certain other law enforcement agencies.

5. The Commission acknowledges the critical importance of ensuring that our police and security agencies have appropriate tools to investigate criminal activity as well as to protect our national security. Human rights law provides significant scope for such agencies to have expansive powers, even where they impinge on individual rights and freedoms. Such limitations must, however, be clearly expressed, unambiguous in their terms, and legitimate and proportionate responses to potential harms.

6. The Commission considers that the Bill goes beyond what can be reasonably justified. We make five recommendations to address concerns about risk to human rights. Without these changes, the Commission would oppose the Bill.

3 Recommendations

7. The Australian Human Rights Commission recommends that:

Recommendation 1: That the data required to be retained be included in the primary legislation.

Recommendation 2: That the Bill be amended to include a definition of 'content'.

Recommendation 3: That an initial retention period of 1 year be trialled for the first 3 years of the scheme's operation.

Recommendation 4: That the Committee review the circumstances in which communications data can be accessed and restrict it to circumstances where it is reasonably necessary for the prevention, detection or prosecution of defined, sufficiently serious crimes.

Recommendation 5: That an independent authorisation system by a court or administrative body be implemented.

8. The Commission notes that if its recommendation 4 is not accepted then recommendation 5 carries a much greater importance.

9. The Commission also considers that there should be penalties for inappropriate access and misuse of data.

4 Human Rights Framework

10. The establishment of a mandatory data retention scheme interferes with the right to privacy under article 17 of the *International Covenant on Civil and Political Rights* (ICCPR). It also indirectly interferes with the right to freedom of expression under article 19 of the ICCPR.

4.1 Article 17 – the Right to Privacy

11. Article 17 of the ICCPR provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

12. Article 17 protects individuals from the collection of their personal information by others, including government. The United Nations Human Rights Committee (HRC) has concluded that the capture of communications data amounts to a *prima facie* interference with privacy:

> [A]ny capture of communications data is potentially an interference with privacy and, further… the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.[2]

13. Any limitation on privacy must be lawful. That means that any limitations on the right must be provided for by law:

> The State must ensure that any interference with the right to privacy…is authorised by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorising, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.[3]

14. Further, any interference with the right to privacy must not be arbitrary. This means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances.[4] Reasonable in this context means any limitation must be proportionate and necessary to achieve a legitimate objective.[5]

15. The Bill's statement of compatibility acknowledges that the mandatory retention of data limits the right to privacy and identifies the legitimate objective of the legislation as being:

> The protection of national security, public safety, addressing crime, and protecting the rights and freedoms of others by requiring the retention of a basic set of communications data required to support relevant investigations.[6]

16. The HRC has recently commented on data retention schemes by stating:

> Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.[7]

17. Further, the Court of Justice of the European Union has recently ruled the European Union Data Retention Directive to be invalid because it disproportionately interfered with the right to privacy and data protection.[8] The EU Data Retention Directive imposed an obligation on Member States to adopt measures to ensure that communication data generated or processed by providers of public communication services or networks within their jurisdiction be retained for six months to two years and stored in such a way that it could be transmitted upon request to the 'competent authorities' without delay. The Court of Justice of the European Union identified several characteristics of the Data Retention Directive that rendered the regime disproportionate. The effect of this was to define the limits of permissible data retention pursuant to human rights law. Relevant limits will be discussed in more detail below.

4.2 Article 19 – Freedom of Expression

18. Article 19 of the ICCPR provides:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

19. The statement of compatibility identifies that a mandatory data retention scheme engages and potentially limits the right to freedom of expression. It notes:

> Requiring providers of telecommunications services to retain telecommunications data about the communications of its subscribers or users as part of a mandatory dataset may indirectly limit the right to freedom of expression, as some persons may be more reluctant to use telecommunications services to seek, receive and impart information if they know that data about their communications will be stored and may be subject to lawful access.[9]

20. The only permissible restrictions on the freedom of expression are those described in paragraph 3 of Article 19.[10] The statement of compatibility states that any limitation is 'designed for the legitimate object of protecting public order',[11] which includes 'preventing crime'.[12] The Commission acknowledges that the prevention and detection of crime may be regarded as a legitimate objective.

21. Any limitation on the freedom of expression must be according to law. Laws limiting the freedom must be made accessible to the public, and must provide sufficient guidance both to those executing the laws, and to those whose conduct is being regulated.[13]

22. Further, any limitation on the freedom of expression must be necessary and proportionate to achieve its legitimate objective.

5 Scope of dataset to be retained

23. Schedule 1 of the Bill proposes to require providers of telecommunication services to retain certain telecommunications data in relation to all communications for a period of two years. The Explanatory Memorandum explains that telecommunications data is information about a communication, such as the phone numbers of the people who called each other, how long they talked to each other, the e-mail address from which a message was sent and the time the message was sent.[14]

24. The categories of data required to be collected and retained by service providers are not specified in the Bill but will be set out in Regulations. The Explanatory Memorandum states that:

> The use of regulations to prescribe the details of data to be retained facilitates the prescription of the necessary technical detail to provide clarity to telecommunications service providers about their data retention obligations while remaining sufficiently flexible to adapt to rapid and significant future changes in communications technology.[15]

25. The Commission acknowledges the rationale for using Regulations. However, the Commission considers that the definition of telecommunications data is a critical feature of the Bill and should not be left to be described by Regulations. The Commission considers that the telecommunications data required to be retained by telecommunication services providers should be included in the legislation itself.

Recommendation 1: That the data required to be retained be included in the primary legislation.

26. Proposed s 187A(2) limits the range of data that may be prescribed by Regulations to specific categories, including information relating to:

    a. The subscriber, accounts, telecommunication devices and other relevant services of a relevant service (s187A(2)(a));

    b. The source of a communication (s187A(2)(b));

    c. The destination of a communication (s187A(2)(c));

    d. The date, time and duration of a communication (s187A(2)(d));

    e. The type of communication (s187A(2)(e));

    f. The location of the line, equipment or telecommunications device (s187A(2)(f)).

27. Proposed ss187A(4)(a) and (b) of the Bill explicitly exclude web browsing history and ‘content’ from the scope of data that may be subject to mandatory retention. The Commission supports these exclusions in the Bill. However, the Commission notes that there is no definition of ‘content’ in the Bill. The

Commission recommends that the Bill be amended to include a definition of 'content' for the purposes of the scheme.

Recommendation 2: That the Bill be amended to include a definition of 'content'.

6 Two year retention period

28. The Commission notes that the proposed retention period of two years is at the upper end of retention periods implemented in comparable jurisdictions.

29. The Explanatory Memorandum states that

> The retention period reflects international experience that, while the majority of requests for access to telecommunications data are for data that is less than 6 months old, certain types of investigations are characterised by a requirement to access data up to 2 years old. These include complex investigations such as terrorism, financial crimes and organised criminal activity, serious sexual assaults, premeditated offences and transnational investigations. Against the particular context of the critical importance of telecommunications data in very serious crime types and security threats, the two year retention period provides a proportionate response to that environment.[16]

30. As outlined above, the EU Data Retention Directive required Member States to establish a data retention regime for between six months and two years. Only one Member State (Poland) specified a two year retention period. One State specified 1.5 years (Latvia), ten specified one year (Bulgaria, Denmark, Estonia, Greece, Spain, France, Netherlands, Portugal, Finland , the United Kingdom) and three specified six months (Cyprus, Luxembourg, Lithuania).[17]

31. An Evaluation Report on the Data Retention Directive in 2011 considered shortening the periods of mandatory retention would improve proportionality of the scheme.[18] The Report also found that 67% of accessed data was under 3 months old; 19% was between 3-6 months old; 12% was 6-12 months old and only 2% was over 1 year old.[19]

32. In the landmark decision of the Court of Justice of the European Union, which invalidated the EU Data Retention Directive, the Court identified several characteristics of the Directive that rendered the regime a disproportionate interference with the rights to privacy. Relevantly, the Court considered that retention periods should be limited to that which is 'strictly necessary'.[20] Further, retention schemes should distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned.[21]

33. The Commission is concerned about the 2 year retention period proposed in the Bill. The Commission notes the evidence from the Evaluation Report on the EU Data Retention Directive in 2011 that only 2% of requested data was over 1 year old across the European Union. The Commission notes that the majority of EU countries (including the United Kingdom) have specified a 1 year retention period.[22] The Commission submits that an initial retention

period of 1 year would be a more proportionate interference with the right to privacy.

Recommendation 3: The Commission recommends that an initial retention period of 1 year be trialled for the first 3 years of the scheme's operation.

7 Access to retained communications data

34. Under the current regime, law enforcement agencies may access historical communications data in circumstances where it is considered reasonably necessary for:

    a. the enforcement of criminal law;[23]

    b. the enforcement of a law imposing a pecuniary penalty;[24] or

    c. the protection of public revenue.[25]

35. Access to prospective communications data, however, may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of an offence with a maximum prison term of at least three years.[26]

36. For ASIO, these authorisations may only be made where the person making the authorisation is 'satisfied that the disclosure would be in connection with the performance by the Organisation of its functions.[27]

37. As outlined above, the Court of Justice of the European Union found that the EU Data Retention Directive was not a proportionate interference with the right to privacy. One of the reasons for this was that it considered that access and use of the data should be restricted to the prevention, detection or prosecution of defined, sufficiently serious crimes.[28]

38. The Commission considers that access to communications data should be restricted to sufficiently serious crimes to warrant the intrusion on the right to privacy.

39. A large number of agencies may currently access communications data without a warrant, including:

    - Australian Federal Police, Australian Commission for Law Enforcement Integrity,
    - Australian Crime Commission
    - Australian Customs and Border Protection Services
    - CrimTrac
    - State and Territory police forces
    - State anti-corruption agencies
    - A body whose functions include administering a law imposing a pecuniary penalty or a law relating to the protection of the public revenue.[29]

The category of pecuniary penalty and public revenue enforcement agencies includes a range of bodies such as:

- Australian Competition and Consumer Commission
- Australian Securities and Investments Commission
- Australian Taxation Office
- Department of Human Services
- Department of Immigration and Border Protection, and
- Local councils[30]

40. Schedule 2 of the Bill proposes to amend the definition of 'enforcement agency' under the TIA Act to confine the number of agencies that are able to access communications data. The listed agencies would include the ASIO, Australian Federal Police, a police force of a State and the Australian Commission for Law Enforcement Integrity. Under proposed s 110A, the Minister would have the power to declare further authorities or bodies to be a 'criminal law enforcement agency'.

41. The Commission supports the Bill's proposal to confine the number of agencies that may access retained telecommunications data. The Commission notes that this is consistent with the Court of Justice of the European Union's decision, which states that the number of persons authorised to access and subsequently use the communications data should be limited to that which is strictly necessary.[31]

42. However, in the Commission's view, the confinement of agencies to criminal law enforcement agencies should also be reflected in the threshold for accessing telecommunications data. The Commission considers that access to historical telecommunications data should only be allowed where it is reasonably necessary for the prevention, detection or prosecution of defined, sufficiently serious crimes.

Recommendation 4: That the Committee review the circumstances in which communications data can be accessed and restrict it to circumstances where it is reasonably necessary for the prevention, detection or prosecution of defined, sufficiently serious crimes.

8 External oversight

43. The TIA Act also sets out who is able to authorise access to retained communications data, being a Head of an agency; the deputy head of any agency; or an officer or employee of the agency covered by an approval, in writing, of the head of the agency.[32] Notably all agencies may access retained communications data without a warrant from an independent body.

44. The Commission notes that the Court of Justice of the European Union considered that an independent administrative or judicial body should make decisions regarding access to the retained communications data on the basis of what is strictly necessary.[33]

45. The current regime allows agencies to access communications data without a warrant but mandates a warrant for access to the content of communications. The Commission considers that a warrant system is necessary for the access to communications data as well. This is especially the case given the question of whether the distinction between content and communications data for the purposes of the right to privacy can be legitimately maintained. The HRC has recently stated:

> It has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.[34]

46. Further, the Court of Justice of the European Union observed that communications metadata:

> Taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[35]

47. The International Principles on the Application of Human Rights to Communications Surveillance, 2013 considers that:

> While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection.[36]

48. Contrary to the claims made in the Explanatory Memorandum,[37] the Commission considers the retention of and access to communications data may not be any less intrusive than retention of and access to content. The requirement to store communications data on each and every customer just in case that data is needed for law enforcement purposes is a significant intrusion on the right to privacy and justifies a warrant system for access to it.

49. Further, requiring a warrant to access metadata is not without precedent in other countries. In the EU, eleven Member States require judicial authorisation for each request for access to retained data. In three Member States judicial authorisation is required in most cases. Four other Member States require authorisation from a senior authority but not a judge.[38]

50. The Commission notes that certain oversight measures are included in the Bill, including

a. the Commonwealth Ombudsman oversight of the mandatory retention scheme; and

b. the Parliamentary Joint Committee on Intelligence and Security's proposed review of the scheme three years after the conclusion of the implementation phase.

51. The Commission notes that the Inspector-General of Intelligence and Security will continue to oversight access to telecommunications by ASIO. The Privacy Commissioner will continue to assess industry's compliance with the Australian Privacy Principles as well as monitoring industry's non-disclosure obligations under the Telecommunications Act.

52. While these safeguards are important checks on the scheme, they are all directed at reviewing access powers after they have been exercised. The Commission considers that a warrant or authorisation system for access to retained data by a court or administrative body provides a more effective safeguard to ensure that the right to privacy is only limited where strictly necessary.

Recommendation 5: That an independent authorisation system by a court or administrative body be implemented

53. The Commission notes that if its recommendation 4 is not accepted then recommendation 5 carries a much greater importance.

54. The Commission also considers that there should be penalties for inappropriate access and misuse of data.

---

[1] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). At http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx (viewed 19 August 2014).
[2] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (2014), [20].
[3] See *Weber and Saravia v Germany*, application no. 54934/00, 29 June 2006.
[4] UNHRC, *General Comment 16* (1988) U.N. Doc. HRI/GEN/1/Rev.1 at 21, [3], [4].
[5] *Toonen v Australia* UN Human Rights Committee Communication No. 488/1992.
[6] Statement of Compatibility, 10 [33].
[7] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (2014), [26].
[8] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014), [69].
[9] Explanatory Memorandum, 28.
[10] UNHRC, *General Comment 34*, (2011), UN Doc. CCPR/C/GC/34, [22].
[11] Explanatory Memorandum, 29.
[12] Explanatory Memorandum, 28.
[13] UNHRC, *General Comment 34*, (2011), UN Doc. CCPR/C/GC/34, [25].
[14] Explanatory Memorandum, 2 [3].
[15] Explanatory Memorandum, 7 [13].

[16] Explanatory Memorandum, 18 [71].
[17] European Commission, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.3.2011 COM (2011) 225 final, 14.
[18] European Commission, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.3.2011 COM (2011) 225 final, 32.
[19] European Commission, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.3.2011 COM (2011) 225 final 22.
[20] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014), [64].
[21] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014), [63].
[22] *Data Retention and Investigatory Powers Act 2014*, s 1(5).
[23] *Telecommunications (Interception and Access) Act 1979,* s 178.
[24] *Telecommunications (Interception and Access) Act 1979,* s 179.
[25] *Telecommunications (Interception and Access) Act 1979,* s 179.
[26] *Telecommunications (Interception and Access) Act 1979,* s 180.
[27] *Telecommunications (Interception and Access) Act 1979,* s 175 & 176.
[28] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014), [60]-[61].
[29] *Telecommunications (Interception and Access) Act 1979*, s 5.
[30] Attorney-General, *Telecommunications (Interception and Access) Act: Report for the year ending June 2013*, Commonwealth of Australia, 45.
[31] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014), [62].
[32] *Telecommunications (Interception and Access) Act 1979,* s 178-180.
[33] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014), [62].
[34] Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* UN Doc A/HRC/27/37 (2014), [19].
[35] *Digital Rights Ireland Ltd (C-293/12) and Karntner Landesregierung ors (C-594/12) v Minister for Communications, Marine and Natural Resources and ors* (8 April 2014), [27].
[36] *International Principles on the Application of Human Rights to Communications Surveillance*, 2013, 2,. available at: https://en.necessaryandproportionate.org/ (accessed 9 December 2014).
[37] See for example Explanatory Memorandum, 3 [10] and 5 [5].
[38] European Commission, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.3.2011 COM (2011), 9-11.