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

Submission to the Parliamentary Joint Committee on Intelligence and Security

19 January 2015

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Contact

Hugh de Kretser and Emma Newnham
Human Rights Law Centre Ltd
Level 17, 461 Bourke Street
Melbourne VIC 3000

T: + 61 3 8636 4420
F: + 61 3 8636 4455
E: Hugh.deKretser@hrlc.org.au
W: www.hrlc.org.au

About the Human Rights Law Centre

The Human Rights Law Centre is an independent, non-profit, non-government organisation that protects and promotes human rights in Australia and in Australian activities overseas, through a strategic combination of research, advocacy, litigation and education.

The HRLC is a registered charity and has been endorsed by the Australian Taxation Office as a public benefit institution. All donations are tax deductible.

Follow us at http://twitter.com/rightsagenda
Join us at www.facebook.com/pages/HumanRightsLawResourceCentre

Contents

1. Executive summary

1. The Human Rights Law Centre (**HRLC**) welcomes the opportunity to make this submission on the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Cth) (**Bill**).

2. The Bill proposes to require telecommunications service providers to retain certain metadata for a period of two years. Such a requirement carries significant human rights risks.

3. The collection and retention of metadata can be an effective and useful measure for legitimate law enforcement and national security purposes. The mass metadata collection and retention proposed by this Bill, however, has not been justified. Neither the Bill nor the *Telecommunications (Interception and Access) Act 1979* (Cth) (**Act**) contain adequate safeguards against the significant risk of privacy breaches.

4. In particular, the HRLC is concerned that:

   (a) there is no warrant or other similar independent approval process prior to access by enforcement agencies to stored metadata;

   (b) the two year retention period has not been justified;

   (c) access to personal metadata for minor or trivial law enforcement offences is not justified and there is no requirement to disclose or record the relevant offence prior to obtaining access;

   (d) the data types required to be collected and stored by telecommunications service providers are located in regulations, rather than the primary legislation, which raises concerns about arbitrary and unlawful "scope creep"; and

   (e) other key aspects of the data retention scheme have not been detailed in the Bill, which is unsatisfactory given the significant interference mandatory metadata retention will have on the right to privacy.

5. In its current form, the data retention scheme creates a significant risk that Australia will violate international human rights law.

6. The HRLC recommends that the Bill not be passed.

Recommendation: **That the Bill not be passed.**

2. Human rights engaged

2.1 Overview

7. The proposed reforms raise concerns regarding Australia's international law obligations to respect, protect and fulfil the human rights, in particular the rights set out in the International Covenant on Civil and Political Rights (**ICCPR**). The following rights, among others, are engaged by the proposed reforms:

   (a) the right to privacy (article 17);

   (b) the right to freedom of opinion and expression (article 19); and

   (c) the right to an effective remedy (article 2(3)).

2.2 Right to privacy

8. The right to privacy is set out in article 17 of the ICCPR, which provides as follows:

> 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.

9. The right to privacy is not absolute. If the Government wishes to limit the right to privacy, it must state the overriding public interest in limiting the right and establish that the means used are reasonable, necessary and proportionate.

10. It has been suggested that the collection of metadata, as opposed to the content of communications, does not constitute an interference with privacy. In its report on privacy in the digital age (**Privacy Report**), the Office of the United Nations High Commissioner for Human Rights has rejected that suggestion:

> From the perspective of the right to privacy, this distinction [between data about a communication and content] is not persuasive. The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social resolutions, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.[1]
>
> …It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even

[1] This view was adopted in a resolution of the General Assembly adopted on 25 November 2014: see United Nations General Assembly Third Committee, *The right to privacy in the digital age*, 69th sess, UN Doc A/C.3/69/L.26/Rev.1 (19 November 2014), p 3.

> the mere possibility of communications information being captured creates an interference with privacy…"[2]

11. In a joint case in April last year (**Digital Rights**),[3] the European Court of Justice found that the data required to be collected and retained under the European Union Data Retention Directive (**Directive**), which is of a similar nature to the proposed data set released with the Bill, when 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.[4]

12. And further:

> The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by [the Directive], directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the [Charter of Fundamental Rights of the European Union (**European Charter**)].

13. Article 7 of the European Charter provides that everyone has the right to respect for his or her private and family life, home and communications. The Court concluded that the obligation imposed by the Directive on communications providers to retain data relating to a person's private life and communications constitutes "in itself" an interference with the rights guaranteed by article 7 of the European Charter.[5]

14. The Court found that, in order to limit the interference to that which is strictly necessary, the Directive would need to:

> lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data…[6]

---

[2] Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, 27th sess, UN Doc A/HRC/27/37 (30 June 2014) at [19].

[3] Joined cases *Digital Rights Ireland Ltd v Minister for Communications and anor* (European Court of Justice, C-293/12, 8 April 2014) and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others (European Court of Justice, C-594/12, 8 April 2014).

[4] Ibid, at [27].

[5] At [34].

[6] At [54].

15. The Court relied on the following aspects of the Directive to find that it was not sufficiently circumscribed to ensure that it was limited to what was strictly necessary:

(a) the general absence of limits on the requirement to retain data, including limits on the means of electronic communication, and the persons covered;

(b) the failure to set out objective criteria to restrict national authorities' access and use of the data to the purpose of preventing and detecting "precisely defined serious offences" or of conducting criminal prosecutions;

(c) the failure to set out objective criteria for limiting the number of persons authorised to access and use the data to what is strictly necessary;

(d) the requirement to retain the data for a period of at least 6 months, regardless of the category of data and possible usefulness for criminal enforcement purposes and regardless of the persons concerned; and

(e) "above all," the access by national authorities not being made dependent on a prior review carried out by a court or independent administrative body.[7]

16. The Privacy Report goes further, providing that mandatory and indiscriminate third-party data retention may never be necessary or proportionate:

> 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."[8]

17. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, takes a similar view:

> In the view of the Special Rapporteur, the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy. Shortly put, it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. The very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis...[9]

[7] At [57]-[65].

[8] At [26].

[9] Special Rapporteur, *Promotion and protection of human rights and fundamental freedoms while countering terrorism*, 69th sess, UN doc A/69/397 (23 September 2014) at [18]. Footnotes omitted.

18. There is therefore a heavy onus on the Australian government to explain "promptly, precisely and publicly why this wholesale intrusion into collective privacy is justified for the prevention of terrorism or other serious crime."[10]

19. If the intrusion can be justified, the Australian government must ensure that appropriate safeguards are in place to ensure that the interference is sufficiently circumscribed to ensure that the right to privacy is interfered with only so far as is strictly necessary. In particular:

> The State must ensure that any interference …is authorized 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 authorizing, 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.[11]

2.3 Right to freedom of opinion and expression

20. The right to freedom of opinion and expression is contained in article 19 of the ICCPR:

> 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.

21. Article 19(3) provides that this right can be subject to certain restrictions, where they are provided by law and necessary for the respect of the rights or reputations of others or for the protection of national security, public order, public health or morals.

22. The European Court of Justice acknowledged in the Digital Rights case that the freedom of expression may be engaged by mass metadata retention laws as such laws may effect the use of the means of communication falling within their scope.[12]

[10] At [19].

[11] Privacy Report, at [28]. A footnote in the source refers to CCPR/C/USA/CO/4, para. 22. See also European Court of Human Rights, Malone v the United Kingdom, No. 8691/79, 2 August 1984, paras. 67 and 68; and Weber and Saravia v Germany, application no. 54934/00, 29 June 2006, in which the Court lists minimum safeguards that should be set out in statute law.

[12] At [28].

23. According to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression:

> Communications surveillance[13] should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.[14]

2.4 Right to an effective remedy

24. The right to an effective remedy is set out in article 2(3) of the ICCPR:

> Each State Party to the present Covenant undertakes:
>
> (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;
>
> (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;
>
> (c) To ensure that the competent authorities shall enforce such remedies when granted.

3. Interference not sufficiently circumscribed

3.1 Overview

25. Even if the Australian government were able to justify the introduction of a mass data retention scheme, this Bill does not sufficiently circumscribe the intrusion on human rights so that it is strictly necessary, or proportionate, for law enforcement and national security purposes.

26. On the contrary, the Bill fails, despite calls by other committees and organisations in recent years, to put in place important and meaningful safeguards on the retention of, and access to stored, metadata.

[13] Defined by the Special Rapporteur to include the collection and retention of information that has been communicated, relayed or generated over communications networks (at [6]).

[14] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 23rd sess, UN Doc A/HRC/23/40 (17 April 2013).

3.2 Absence of supervision by independent judicial authority

27. Neither the Bill nor the Act currently require a warrant or other authorisation by an independent judicial authority for access to, and use of, stored metadata.

28. A warrant or other similar prior approval process is necessary to ensure that issues of privacy are considered by an independent authority[15] and that there is sufficient evidence to avoid a fishing expedition. The warrant or other prior approval process should also require consideration of whether access and use is strictly necessary for the purposes of law enforcement and national security.

29. The lack of an independent prior approval requirement in the current authorisation process increases the risk of abuse by government and non-government entities. In the November 2013 surveillance scandal, Federal Police Commissioner Tony Negus admitted that up to five MPs had been the subject of data surveillance without a warrant. According to some commentators, the data requests may have targeted MPs who had leaked information to the media,[16] potentially constituting an arbitrary interference with the MPs privacy.

30. The absence of a warrant or other independent authorisation process prior to access and use of the stored data gives rise to serious concerns regarding the propriety, and apparent propriety, of the access and use. As the Privacy Report notes:

> Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires."[17]

31. We note that the Parliamentary Joint Committee on Human Rights raises similar concerns in relation to the lack of prior review and recommends the Bill be amended to provide that access be granted only following a warrant approved by a court or independent administrative tribunal.[18]

32. A warrant or similar prior approval process should also provide a mechanism for individuals to be notified and have the opportunity to challenge the legality of access to their telecommunications data. Notification could occur after access where ex parte approval was

[15] Cf section 180F of the Act which requires an authorised officer of the agency, when considering an authorisation, to consider certain matters including privacy.

[16] Ross Coulthart, 'Australia's real surveillance scandal', *The Global Mail* (online), 13 December 2013 <http://www.theglobalmail.org/feature/australias-real-surveillance-scandal/777/>.

[17] At [37]-[38].

[18] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011: Fifteenth Report of the 44th Parliament* (2014) at [1.59].

necessary for law enforcement or national security purposes. This process should mitigate the concern that the right to an effective remedy is being impermissibly interfered with because individuals are unable to challenge decisions or applications in relation to their stored metadata because they are never informed of the decisions or applications.

3.3 Two year retention period not justified

33. At the public hearing on 17 December 2014, ASIO acknowledged that around 90% of requests to access stored metadata were for periods of less than 12 months.[19] The international experience was said to be similar, with about 75% of data sought usually six months old or less, and around 90 or 95% one year old or less.[20]

34. Other evidence given at the hearing suggests only one other country in the world has legislation requiring internet data to be retained for two years or more: South Africa.[21]

35. A blanket two year retention period for all means of communication will mean that, at any time, vast amounts of private information about individuals is held by telecommunications service providers. Such information will be at risk of unauthorised access or misuse; serious consequences could flow from a security breach.

36. The Inquiry into Potential Reforms of National Security Legislation recommended that the retained data should be stored securely by making encryption mandatory.[22] The government has promised to establish a security framework for the telecommunications sector,[23] but this is not included in the Bill.

37. Unless and until proper safeguards for the stored data are put in place, including effective security arrangements, a sufficient case for a two year retention period cannot be made.

3.4 Access to data for minor offences

38. The explanatory memorandum points out that, where the Minister declares an authority to be an enforcement agency or a criminal law enforcement agency, the Minister will be able to limit

[19] Evidence to Parliamentary Joint Committee on Intelligence and Security, Commonwealth of Australia, Canberra, 17 December 2014, p 5 (Ms Hartland).

[20] Evidence to Parliamentary Joint Committee on Intelligence and Security, Commonwealth of Australia, Canberra, 17 December 2014, p 21 (Mr Clare).

[21] Evidence to Parliamentary Joint Committee on Intelligence and Security, Commonwealth of Australia, Canberra, 17 December 2014, p 20 (Mr Clare).

[22] Parliamentary Joint Committee on Intelligence and Security, Parliament of the Commonwealth of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, 2013, p 192.

[23] Australian Government, *Data Retention Facts: Keeping our community safe* < http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/KeepingourcommunitysafeFactsheet.pdf>.

the authority's status as an enforcement agency or criminal law enforcement agency to offences with a three year or more imprisonment term, or offences with more significant penalties.[24]

39. In the absence of such a limitation, enforcement agencies can access stored metadata regardless of the gravity of the offence. The only requirements are that an authorised officer of the agency is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law (or other specified aims), and has considered whether any interference with privacy is justifiable.[25] As noted by the Parliamentary Joint Committee on Human Rights, there appears to be no restriction on access to stored metadata in the Bill based on the nature or seriousness of the offence.[26]

40. The failure to set out objective criteria restricting access and use of data for the purpose of preventing and detecting carefully defined serious offences or of conducting criminal prosecutions was one of the key criticisms levelled at the Directive in the Digital Rights decision.

41. The same criticism was raised in Germany in relation to legislation intended to implement the Directive into German law. The legislation was found to be disproportionate and unconstitutional, in part because the stored data could be accessed for a wide variety of purposes, rather than strictly for the investigation of serious crimes.[27]

42. The Bill should establish a gravity threshold so that retained metadata can be accessed and used only where it is necessary for investigating serious crimes; not minor or trivial offences.

3.5 Data types not provided in primary legislation

43. The Court in the Digital Rights case found that, in order to limit the interference to that which is strictly necessary, the relevant legislation would need to lay down "clear and precise rules governing the scope and application of the measure in question."[28]

[24] At [204] and [221]. And see schedule 2, items 2 and 4 of the Bill.

[25] Part 4-1 of the Act.

[26] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011: Fifteenth Report of the 44th Parliament* (2014) at [1.48].

[27] Bundesverfassungsgericht, Judgement 02. March 2010, 1 BvR 256/08. The decision is available in German here: <http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html>. See also the Law Council's submission to the Parliamentary Joint Committee on Intelligence and Security's Inquiry into Potential Reforms of Australia's National Security Legislation, *Submission No. 224*, pp 9-10.

[28] At [54].

44. Although the categories of data required to be retained are set out in the legislation, the types of data falling within those categories is proposed to be left to regulations made pursuant to proposed section 187A(1)(a).

45. Leaving this integral part of the scheme to regulations reduces the control and oversight of parliament over changes to the scheme and increases the risk of arbitrary and unlawful changes that increase the scope of the scheme.

46. The Privacy Report notes that:

> Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights.[29]

47. Article 25 of the ICCPR protects an individual's right and opportunity to take part in the conduct of public affairs.

48. We note that the Senate Standing Committee for the Scrutiny of Bills also recommends that consideration be given to amending the Bill to include the types of data required to be collected and stored.[30]

3.6 Other key aspects of the data retention scheme not detailed in Bill

49. In addition to the type of data covered by the Bill, certain other aspects of the retention scheme have been left out of the Bill. In particular, the Bill allows the Minister to declare additional authorities or bodies to be criminal law-enforcement agencies[31] and enforcement agencies.[32]

50. The replacement of the current definition of "enforcement agency" with a definition intended to limit the number of agencies able to access telecommunications data is a positive step. The current definition includes broad catch-all descriptors extending, for example, to any body whose functions include administering a law imposing a pecuniary penalty.[33] The existing broad definition could potentially extend to a large number of bodies (including, for example,

[29] At [29]. The footnote in the source provides: see also A/HRC/14/46.

[30] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Alert Digest No. 16 of 2014* (26 November 2014) p 4.

[31] Schedule 2, item 3, clause 110A(3) of the Bill.

[32] Schedule 2, item 4, clause 176A(3) of the Bill.

[33] Section 5(1) of the Act.

local councils) and there is no mechanism for determining which bodies or authorities fall within the current definition. The new definition is said to "rectify this concern" by specifying a list of criminal law-enforcement agencies with power for the Minister to declare additional authorities or bodies to be criminal law-enforcement agencies or enforcement agencies.[34]

51. However, rather than rectifying the problem, this broad Ministerial power introduces further uncertainty and leaves important aspects of the Bill to be finalised after the legislation has been introduced, and therefore without parliamentary oversight.

52. We have had the benefit of reading the submission by the Gilbert + Tobin Centre of Public Law dated 9 December 2014 and support the views expressed in section 2 of that submission.

4. Conclusion

53. The collection and retention of metadata can be an effective and useful measure for legitimate law enforcement and national security purposes.

54. This Bill, however, exposes an unlimited number of people, who are not suspected of any wrongdoing, to risks of improper access and use of their personal data without their permission or even knowledge.

55. The extent of this interference with their privacy has not been shown to be necessary for law enforcement or national security purposes and, when combined with the lack of appropriate safeguards, presents an impermissible interference with international human rights.

56. The Bill should not be passed.

Recommendation: **That the Bill not be passed.**

[34] Explanatory memorandum to the Bill, at [216].