Review of the mandatory data retention regime

Submission to the Parliamentary Joint Committee on Intelligence and Security

12 July 2019

www.hrlc.org.au

Freedom. Respect. Equality. Dignity. Action.

Contact

Alice Drury (Lawyer) and Emily Howie (Legal Director)

Human Rights Law Centre
Level 17, 461 Bourke Street
Melbourne VIC 3000

T: + 61 3 8636 4474
F: + 61 3 8636 4455
E: alice.drury@hrlc.org.au
W: www.hrlc.org.au

Human Rights Law Centre

The Human Rights Law Centre uses a strategic combination of legal action, advocacy, research, education and UN engagement to protect and promote human rights in Australia and in Australian activities overseas.

It is an independent and not-for-profit organisation and donations are tax-deductible.

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

Contents

1. Executive Summary

1. Thank you for the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's (**Committee**) review of the mandatory data retention regime contained in Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**). This submission was drafted by the Human Rights Law Centre and is endorsed by Access Now and Digital Rights Watch.

2. The reality of today's metadata retention regime bears little resemblance to the context in which this Committee reviewed the scheme in 2015. At that time, the regime was expected to be used sparingly, for the investigation of serious crimes by a limited number of agencies.

3. Instead, we have a system of widespread access that extends to investigation of minor offences. Over 80 government agencies have requested access to metadata. Agencies such as the oversight bodies for the racing industry and taxi services are contributing to the 350,000 requests for access to metadata made each year.[1] Media reports indicate that local councils have accessed metadata to pursue unpaid fines and enforce minor infringements, including for littering.[2]

4. In 2015, it was accepted that access to metadata was less intrusive than access to the content of communications. The opposite is now well understood – metadata allows precise conclusions to be drawn about peoples' private lives and is no less sensitive than content of communications.

5. During the intervening period, we have also seen the expansion of surveillance powers in Australia and the criminalisation of speech in an increased range of circumstances. Since 2015, Parliament has:

   (a) Passed world-first legislation allowing law enforcement agencies to access encrypted communications in the investigation of relatively minor offences (*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (**TOLA**).

   (b) Passed amendments to the *Criminal Code* that significantly broaden espionage, secrecy, sabotage and foreign interference offences so far, that they could effective criminalise public interest whistleblowing, journalism and protest.

[1] Stanton, J, before the Parliamentary Joint Committee on Intelligence and Security, review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Cth), Canberra, 19 October 2018.

[2] Alexander, Harriet, "Councils pry into residents' metadata to chase down fines" *Sydney Morning Herald*, 15 November 2015, accessed 25 June 2019, available at <https://www.smh.com.au/business/consumer-affairs/councils-pry-into-residents-metadata-to-chase-down-fines-20181114-p50fxr.html>.

(c) Considered proposed legislation enhancing facial recognition capabilities, and is scheduled to again. These laws would allow the Government to develop a database of images of all Australians, facilitating the live tracking of citizens.

6. These recent laws and proposed laws favour broad expansion of surveillance powers, without a correlating increase in safeguards to protect individual rights, or the free press or to guard against mission creep by authorities. The result has been disproportionate and relatively unchecked power in the hands of many authorities, extending beyond law enforcement and intelligence agencies.

7. In just one year, the AFP accessed the metadata of journalists over 60 times.[3]

8. The imbalance in our system was illustrated by the June 2019 Australian Federal Police raids on the home of Daily Telegraph journalist Annika Smethurst and the ABC's headquarters. For years there has been a worrying trend of police investigating and prosecuting whistleblowers who have disclosed government wrong-doing in the public interest.[4] The June raids demonstrated that authorities will investigate journalists too.

9. On 25 June of this year, Australia told the UN Human Rights Council of its commitment to protecting Australians' privacy through safeguards on access to telecommunication data:[5]

> We are committed to maintaining a comprehensive framework for the protection of individuals' personal information. This includes appropriate safeguards and oversight mechanisms to ensure law enforcement and security agencies' access to telecommunications data is subject to strict accountability and oversight.

10. Unfortunately, the reality in Australia does not reflect this commitment. The TIA Act has exposed Australians to arbitrary and unlawful breaches of their privacy and freedom of expression and opinion. Journalists have had their metadata unlawfully accessed without a warrant.

11. Based on international and comparative jurisprudence and commentary, a scheme with the appropriate safeguards would have the following features.

(a) **Limited collection of data.** Data should not be collected from all persons, but only where there is evidence of a person's link with serious crime.

[3] Bevan Shields, "Federal Police accessed the metadata of journalists nearly 60 times," The Age, 9 July 2019, https://www.theage.com.au/politics/federal/federal-police-accessed-the-metadata-of-journalists-nearly-60-times-20190708-p52598.html.

[4] We note the prosecutions against: Witness K and Bernard Collaery for disclosing reprehensible conduct by the Australian Government against Timor L'este; Richard Boyle for revealing misconduct within the ATO; the prosecution of Defence Force lawyer David McBride for leaking information regarding extrajudicial killings carried out by the Australian Defence Force.

[5] 41st session, Australian Human Rights Council, *Clustered Interactive Dialogue with the Special Rapporteur on freedom of expression and the Special Rapporteur on the rights to peaceful assembly and association*, 25 June 2019.

(b) **Limited access based on seriousness of offence**. Access to retained data should be restricted to a small number of agencies responsible for sufficiently serious crimes.

(c) **Independent review of access**. Access to retained data should be made dependent on a prior review carried out by a court or independent administrative decision body.

(d) **Shortest possible retention period**. The data retention period should be based on objective criteria to ensure that it is limited to what is strictly necessary.

(e) **Notification to person affected**. A person should be notified where their metadata has been accessed.

12. Australia's regime falls short of each of these requirements insofar is it:

(a) Requires the indiscriminate collection of all of our data, not only the data of those suspected of committing a crime.

(b) Allows broad access to retained data, without properly limiting the agencies who have access or ensuring that access is sought in connection with sufficiently serious crimes.

(c) Allows warrantless access to information, except journalist information.

(d) Requires data to be held for two years without any justification for that length of time.

(e) Does not provide any notice to a person whose metadata is accessed.

13. We urge the Committee to recommend the amendments below that would go a significant way ensuring we get the balance right and protect peoples' privacy.

2. Recommendations

Recommendation 1: Limit data that is retained

That data only be retained in relation to persons linked with the commission of a serious crime.

Recommendation 2: Limit access to retained data, by agency and seriousness of offence

That access to metadata be confined to:

- a limited number of law enforcement agencies named in the TIA Act; and
- only for the purposes of preventing or investigating specific serious crimes, such as murder, sexual assault, terrorism or organised crime.

With respect to national security offences, we recommend that the TIA Act not permit access to a person's metadata for the new national security offences of espionage, sabotage, secrecy and foreign interference insofar as they criminalise conduct such as journalism in the public interest.

That sections 280 and 313 of the *Telecommunications Act 1997* (Cth) be immediately amended to stop state and government agencies from using their own powers to access metadata and ensure that access is strictly limited to the law enforcement agencies listed in the TIA Act.

Recommendation 3: Require a warrant for access

The TIA Act should require a judicial warrant or warrant issued by an independent authority for access to metadata in all instances.

Recommendation 4: Prohibit access to journalist and public interest whistleblower metadata, except in limited circumstances

That law enforcement agencies be prohibited from accessing the metadata of whistleblowers, journalists, human rights defenders and activists who, in the legitimate course of their work, disclose government wrongdoing in the public interest. A limited exception to this prohibition could allow law enforcement agencies to access their metadata, with a warrant, if necessary to prevent or mitigate an imminent threat to a person's safety.

Recommendation 5: Limit time period in which data is retained

The mandatory two year retention period for companies holding metadata be reduced to the minimum period reasonably required for investigations.

Recommendation 6: Provide notice to peoples whose metadata is accessed

That persons whose metadata is accessed be given notice of such access occurring.

3. Impact on free speech and privacy

14. The TIA Act engages the following rights set out in the *International Covenant on Civil and Political Rights* (**ICCPR**):

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

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

15. The relevant question for determining whether the metadata retention scheme is lawful, is whether the limitations on those rights are reasonable, necessary and proportionate to achieving a legitimate purpose – in this case the prevention of crime and the protection of Australia's national security.

3.1 The right to privacy

16. Article 17 of the ICCPR aims to protect individuals from any unlawful and arbitrary interferences with their privacy, family, home or correspondence, and national legal frameworks must provide for the protection of this right.

17. The Replacement Explanatory Memoranda to the TIA Act suggests that access to metadata "infringes less on personal privacy compared to other covert investigative methods as it does not include the content or substance of the communication".[6]

18. International law and opinion is now clear that metadata is no less sensitive than the content of communications. In *Tele2*, the European Court of justice concluded that:

> That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, 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. In particular, that data provides the means…of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications. [citations omitted]

19. The court also stated that an obligation on telecommunications providers to retain data relating to a person's private life and communications constituted "in itself" an interference with the right to privacy.[7]

3.2 The right to freedom of opinion and expression and a free press

20. The European Court of Justice has recognised that metadata retention laws engage the right to freedom of expression under article 11 of the Charter of Fundamental Rights of the European Union (**Charter**).[8]

21. In its 2015 decision,*Tele2 Sverige AB v Post-och telestyrelsen and SSHD v Tom Watson and Others,*[9] the ECJ observed that just the fact of retaining people's data without informing them is likely to discourage people from using electronic means to communicate.[10] Further, these measures normalise government surveillance over citizens, which has a chilling effect on criticism of the government.

---

[6] Replacement Explanatory Memorandum, *Telecommunications (Interception and Access) Act 1979* (Cth), at [20]. This was supported by Attorney-General's Department, Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* Submission 27, 18.

[7] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [99]. See also Human Right Council, 23rd Session, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17 April 2013, A/HRC/23/40, [42].

[8] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12) and *Kärntner Landesregierung* (C 594/12) [2014] ECR, [28].

[9] (C-203/15) and (C-698/15), [2016] ECR.

[10] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [100].

22. Additionally, the UN Human Rights Committee recommended that States respect the right of freedom of expression by embracing the journalistic privilege not to disclose information sources.[11]

23. The UN expert on free speech said that privacy is an essential requirement for the realisation of the right to freedom of expression, as "undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas".[12]

3.3 Rights-consistent principles of metadata retention

24. Out of the international and comparative jurisprudence it is possible to derive the following propositions for how a metadata retention regime can strike the balance between genuine preservation of public safety and the rights of individuals and a free press.

(a) **Limited collection of data.** Data should not be collected from all persons using electronic communications services, but only where there is evidence capable of suggesting that a person's conduct might have a link, even an indirect or remote one, with serious crime.[13] The retention of data should be the exception and not the rule – the retention should be strictly necessary, and general and indiscriminate data collection is not allowed.[14]

(b) **Limited access based on seriousness of offence**. National laws should set out the procedural and substantive conditions under which access is granted to retained data.[15] Access to retained data should be restricted to the prevention, detection or prosecution of defined, sufficiently serious crimes.[16]

[11] UN Human Rights Committee, 102nd Session, General Comment No 34, 12 September 2011, CCPR/C/GC/34, at [45] and [23].

[12] Human Right Council, 23rd Session, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 17 April 2013, A/HRC/23/40, at [24].

[13] *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), at [58].

[14] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [104] and [108].

[15] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [118].

[16] *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), at [60]-[61]. *Secretary of State for the Home Department v Watson* [2018] EWCA Civ 70.

(c) **Independent review of access**. Access to retained data should be made dependent on a prior review carried out by a court or independent administrative decision body whose decision limits access to what is strictly necessary for the purpose.[17]

(d) **Shortest possible retention period**. The data retention period should be based on objective criteria to ensure that it is limited to what is strictly necessary.[18]

(e) **Notification to person affected**. A person should be notified where their metadata has been accessed.[19]

25. The metadata retention regime was introduced on the promise that it had been carefully drafted to protect privacy and expression and that the circumstances in which agencies may access metadata and impose criminal penalties for the misuse of such information "are strictly controlled under existing legislation".[20]

26. However, our metadata regime clearly does not meet the useful criteria set out by the courts. In Australia, telecommunications and internet service providers are required to maintain all communications data of all users in Australia. Further, Australian law enforcement authorities can access retained data regardless of whether they are fighting serious crime, without prior supervision by a court or independent body and without notifying a person that their data is being accessed.

27. These issues are discussed in turn below.

[17] *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), at [62]. *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [125]. *Secretary of State for the Home Department v Watson* [2018] EWCA Civ 70

[18] *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), at [64].

[19] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [121].

[20] Attorney-General's Department, Parliamentary Joint Committee on Intelligence and Security, *Review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* Submission 27, 6.

4. Restoring the democratic balance

4.1 Data collection should not be indiscriminate

28. Data should not be collected from all persons using electronic communications services, but only where there is evidence capable of suggesting that a person's conduct might have a link, even an indirect or remote one, with serious crime.[21]

29. In Australia, telecommunications and internet service providers are required to maintain all communications data of all users in Australia for two years. It is general and indiscriminate data collection of the kind that the European Court of Justice has found to be a "far-reaching and serious" infringement on the right to privacy, and also detrimental to freedom of expression.

4.2 Access to data should be restricted to investigating genuinely serious crimes, by a select few law enforcement agencies

30. The metadata retention scheme was justified by the Government on the basis that it was central to the investigation of *serious crimes* such as murder, serious sexual assaults, organised crime, terrorism and threats to national security.[22] Furthermore, the TIA Bill was meant to better protect the right to privacy by reducing the number of agencies that could access telecommunications data to only those that "have a clear and scrutinised need for access… and are subject to appropriate privacy and oversight arrangements".[23] This would include a select few "traditional" law enforcement agencies, such as the police, Customs, crime commissions and anticorruption bodies.[24]

31. Unfortunately in practice, the metadata retention scheme has been used by many dozens of agencies to pursue minor infringements.

32. There is no proper threshold relating to the seriousness or nature of the offence to limit access to data. In establishing the offences for which metadata may be accessed, the TIA Act does not make any reference to preventing, detecting or prosecuting "serious crime". Instead, it

[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), at [58].

[22] Turnbull, M, Hansard, House of Representatives, *Second Reading Speech*, 30 October 2014, 12560.

[23] Replacement Explanatory Memorandum, *Telecommunications (Interception and Access) Act 1979* (Cth), at [96].

[24] Turnbull, M, Hansard, House of Representatives, Second Reading Speech, 30 October 2014, 12560. Mr Turnbull also noted that the Bill would grant the Attorney-General the power to declare additional agencies, but only after considering a range of strict criteria, including whether the agency is subject to a binding privacy scheme. We are not aware of any such declarations having been made since the passage of the TIA Act.

extends access for offences that impose pecuniary penalties or protect public revenue.[25] The Parliamentary Joint Committee on Human Rights concluded that the "lack of a threshold, relating to the nature and seriousness of the offence for access to retained data appears to be a disproportionate limitation on the right to privacy".[26] Media reports indicate that local councils have accessed metadata to pursue unpaid fines and enforce minor infringements, including for littering.[27]

33. Furthermore, access to data is not limited to law enforcement and intelligence agencies, but extends to many agencies. The Communications Alliance, the peak telecommunications industry group representing many of the service providers required to comply with the metadata retention regime, has submitted[28] that State and local government agencies are accessing metadata retained under the TIA Act via sections 280(1)(b) and 313 of the *Telecommunications Act 1997* (Cth).[29] Section 280(1)(b) allows the "disclosure or use of information or 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.

34. The Communications Alliance lists over 80 government agencies that have, since the TIA Act came into effect, requested access to metadata. Agencies such as the oversight bodies for the racing industry and taxi services are contributing to the 350,000 requests for access to metadata made to Communications Alliance members per year.[30]

35. The reality of how the metadata retention regime operates now bears little resemblance to the context in which this Committee reviewed the scheme in 2015. At that time, this Committee concluded that only agencies investigating "serious contraventions" of the law should gain access to metadata without a warrant.[31] This Committee trusted that only the 20 agencies listed in the TIA Act and others declared by the Attorney-General under section 110A would gain access to metadata. On that basis, this Committee deemed it sufficient that the Bill be amended to require that, prior to authorising access to metadata, the authorising officer be

[25] Section 180F *Telecommunications (Interception and Access) Act 1979* (Cth).

[26] Parliamentary Joint Committee on Human Rights, Fifteenth Report of the 44th Parliament, 16.

[27] Alexander, Harriet, "Councils pry into residents' metadata to chase down fines" *Sydney Morning Herald*, 15 November 2015, accessed 25 June 2019, available at <https://www.smh.com.au/business/consumer-affairs/councils-pry-into-residents-metadata-to-chase-down-fines-20181114-p50fxr.html>.

[28] In the context of the 2018 review of *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth).

[29] Communications Alliance, *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (in response to a Question on Notice from the Committee), Submission 87.

[30] Stanton, J, before the Parliamentary Joint Committee on Intelligence and Security, review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Cth), Canberra, 19 October 2018.

[31] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, at [6.23].

satisfied on reasonable grounds that the particular disclosure or use of telecommunications data being proposed is proportionate to the intrusion into privacy.[32]

36. In light of what has eventuated, it is clear that this safeguard is insufficient to protect Australians' right to privacy and freedom of expression and opinion. We recommend, first, that sections 280 and 313 of the *Telecommunications Act 1997* (Cth) be immediately amended so that access to metadata is restricted to the law enforcement agencies listed in the TIA Act, in accordance with the Government's commitment.

37. Second, the scope of the TIA Act must be significantly reduced to apply only to the investigation and prosecution of the serious crimes cited by the Government as justifying the Act, such as murder, serious sexual assaults, organised crime, terrorism and threats to national security. Note that, with respect to national security offences, we recommend that the TIA Act not permit access to a person's metadata for the new national security offences of espionage, sabotage, secrecy and foreign interference insofar as they inappropriately criminalise conduct (such as journalism) in the public interest.

4.3 Judicial warrants should be required for access to metadata

38. The TIA Act does not require agencies to obtain a warrant or other authorisation from an independent judicial authority for access to, and use of, stored metadata, except journalist metadata discussed at 4.4 below. Such an approval process is necessary to ensure the right to privacy is maintained, and to prevent government agencies from arbitrarily accessing people's metadata.

39. In its 2015 Report, this Committee concluded that the imposition that a judicial warrant process would place on the operational effectiveness of agencies was too great.[33] The Committee believed that the safeguards and oversight mechanisms for authorisation of access to data explained above would be sufficient to protect Australians' right to privacy.

40. The unforeseen proliferation of agencies accessing metadata, particularly for minor infringements, is proof that the current safeguards are inadequate for protecting Australians' right to privacy and freedom of expression and opinion. We also note, with concern, the Commonwealth Ombudsman's finding of a number of instances in which access to metadata was authorised without sufficient regard to privacy concerns.[34]

---

[32] Recommendation 25 of the *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*. Now section 180F of the TIA Act.

[33] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, at [6.127].

[34] Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979*, November 2018, 10.

41. The TIA Act should require a judicial warrant or warrant issued by an independent authority for access to metadata in all instances.

4.4 Journalist information warrants should protect journalists and whistleblowers

42. The TIA Act includes the journalist information warrant regime, which was designed to protect the confidentiality of journalists' sources. The TIA Act prohibits agencies from making authorisations to access journalists' or their employers' data for the purpose of identifying a confidential source unless a journalist information warrant is in force.[35]

43. As the Alliance for Journalists' Freedom recently stated, "the relationship of trust between the journalists and their sources is the cornerstone of investigative journalism".[36] The journalist information warrant process is not remotely adequate to protect this relationship.

44. The process for obtaining a warrant is inadequate: it is conducted in secret, without the journalist or their media organisation knowing or, crucially, having a chance to respond. Instead, any public interest arguments against the granting of the warrant are put by a government-appointed public interest advocate.[37]

45. Of further concern is the acknowledgment by the AFP that it unlawfully bypassed the journalist information warrant process altogether in one instance in 2017, when an investigator gained access to the phone records of a journalist in order to identify their source. This admission by the AFP prompted an inquiry by the Commonwealth Ombudsman, who concluded that "a number of officers did not appear to fully appreciate their responsibilities when exercising metadata powers".[38]

46. The journalist information warrants are ineffective in practice for two reasons. First, in many cases it will be possible for a law enforcement agency to find a journalists' source without needing a warrant. They will simply access the suspected whistleblower's metadata (ie by accessing the data of the government department suspected of leaking), rather than accessing the metadata of the journalist they are suspected of speaking to.

47. Secondly, the journalist information warrant process was made largely redundant by the TOLA. The TOLA requires "designated communication providers" to facilitate access to a person's encrypted messaging applications, device or computer when issued with a notice

[35] Section 180H *Telecommunications (Interception and Access) Act 1979* (Cth).

[36] Alliance for Journalists' Freedom, *White Paper for Press Freedom in Australia*, May 2019, 12.

[37] Section 180X *Telecommunications (Interception and Access) Act 1979 (Cth)*.

[38] Commonwealth Ombudsman, *A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979*, October 2017, 1.

from an Australian law enforcement agency. Section 317ZH(1) seems to preserve the journalist information warrant provided in the TIA Act, however it is unclear how such a warrant, which governs metadata, applies in the context of a TOLA notice, which may grant access to the entire device of a journalist.

48. Further, sections 317ZH(4) and (5) then negate and undermine the journalist information warrant. Those sections suggest that any act or thing can nonetheless be requested under TOLA if it would "assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory". So it would seem that a request for technical information (including a journalists' metadata) under TOLA can be made so long as it would assist in, or facilitate the giving of effect to a warrant or authorisation otherwise provided, for example other warrants and authorisations that might be made under the TIA Act or the *Telecommunications Act*.

49. The penalties facing whistleblowers and journalists under the new secrecy and espionage offences in the *Criminal Code* are severe, up to life imprisonment for espionage. The journalist warrant process is a weak mechanism to protect freedom of expression – and our democracy.

50. We believe Australia should be robust in its protection of whistleblowers, reporters, human rights defenders and activists who bravely disclose government wrongdoing. For this reason, we recommend that the TIA Act be amended to create an exclusion whereby the metadata of whistleblowers, journalists, human rights defenders and activists who, in the legitimate course of their work, disclose government wrongdoing in the public interest, cannot have their metadata accessed. An exception to this could allow law enforcement agencies to access their metadata, with a warrant, if necessary to prevent or mitigate an immediate threat to a person's safety.

4.5 The retention period should be substantially reduced

51. The two year retention period for metadata is too long, and out of step with the rest of the world. In 2014, ASIO acknowledged that around 90% of requests to access metadata pertained to data that had been captured within the last 12 months.[39]

52. The two year period should be reduced to the minimum period reasonably required, in view of the experience of investigations requiring access to telecommunications data, the comparative experience in other jurisdictions and the need for proportionality and protection of privacy.

[39] Hartland, K, *Evidence to Parliamentary Joint Committee on Intelligence and Security, Commonwealth of Australia*, Canberra, 17 December 2014, 5.

4.6 Notification to a person affected

53. The mandatory retention scheme does not provide for notification to a person who has had their metadata accessed.

54. Notification is a basic safeguard that allows people to know when their privacy has been intruded upon, or for a journalist, where the confidentiality of their source has been compromised. The European Court of Justice has held that a person should be notified where their metadata has been accessed.[40]

55. Instead, in Australia there is no notification system and it is an offence with a jail term of up to two years for a person to disclose information about the existence of a journalist information warrant or related warrant application process.

56. The regime should be amended to provide for proper notification of people affected.

[40] *Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others* (C-203/15) and (C-698/15), [2016] ECR, at [121].