AUSTRALIAN LAWYERS FOR HUMAN RIGHTS

27 January 2017

PO Box A147
Sydney South
NSW 1235
DX 585 Sydney

alhr@alhr.asn.au
www.alhr.asn.au

Brian Kelleher
Assistant Secretary
Infrastructure Security and Resilience Branch
Department of Communications and the Arts

Canberra
ACT 2600

Anne Sheehan
Assistant Secretary
Communications Security Branch
Attorney-General's Department
3-5 National Circuit
Barton
ACT 2600

By email: CommunicationsSecurity@ag.gov.au

Dear Assistant Secretaries

Access to retained data in civil proceedings

Australian Lawyers for Human Rights (ALHR) thanks you for your invitation of 29 November 2016 to provide this submission in relation to the current review by the Minister for Communications and the Attorney-General of the *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the Advisory Report) from the Parliamentary Joint Committee of Intelligence and Security (the Committee).

1. Introduction

We refer in particular in relation to the prohibition in section 280 (1B)(a) of the *Telecommunications Act 1997* (the TC Act) on civil litigant access to telecommunications data retained for the purpose of complying with the mandatory data retention regime in the *Telecommunications (Interception and Access) Act 1979* (TIA Act). That prohibition, and the related proposed regulation making power in section 280 (1C)(a) to enable provision for appropriate exclusions derive from paragraphs 6.116 and 6.117 of the Committee's Advisory Report.

You have asked:

1. In what circumstances do parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act?
2. What, if any, impact would there be on civil proceedings if parties were unable to access the telecommunications data set as outlined in section 187AA of the TIA Act?
3. Are there particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the *Telecommunications Act 1997* should not apply?

2. Summary

We respond to those questions as follows:

Question 1

1.1 We do not have direct knowledge to enable us to reply to this question.

1.2 The point here is, however, that the mandatory data retention scheme was always claimed by the Government to be purely a targeted and proportional response to perceived security threats and in no way related to civil litigation.

1.3 The question should therefore be irrelevant.

1.4 If the question is not irrelevant to the Government, this indicates that the Government is proposing to: (1) completely change the basis on which the mandatory data retention scheme is operated, and (2) allow the use of data obtained by (legal) surveillance for purposes other than originally intended. This is a matter of serious concern from a privacy and human rights point of view.

1.5 We strongly oppose the use of data retained under the mandatory retention scheme for non-criminal and non-security matters involving civil litigation, where there is no high standard of proof and matters can be decided simply on the balance of probabilities.

Question 2

2.1 If parties to civil litigation were unable to access data which is only collected because it is subject to the TIA mandatory retention requirements, the *status quo* would be retained.

2.2 We believe that this is desirable and indeed that retention of data and access to it should both be restricted, not expanded.

2.3 We acknowledge that it may be difficult for telcos and ISPs to distinguish between data which they would have collected and retained for operational purposes or which they had just not got around to deleting, and data which they only collect and retain because of their TIA obligations. A practical solution might be to set an arbitrary cut off point whereby data not required for operational purposes will not be accessible for the purposes of civil litigation after it is more than 6 months old.

Question 3

We support the retention of the prohibition in section 280 (1B) and answer the third question: 'No. The Prohibition in section 280(1B) of the *Telecommunications Act 1997* should apply to all civil proceedings.'

Recommendations

We also endorse the recommendations of Electronic Frontiers Australia[1] that:

- There should be no expansion of access to retained telecommunications data for any civil proceedings;
- The government should instigate an urgent review into the efficacy of the Mandatory Data Retention Scheme during 2017;
- The government should ensure that a comprehensive and adequate data breach notification scheme is introduced without further delay;
- The government should instigate a parliamentary committee to consider the introduction of a statutory cause of action for serious invasions of privacy (a 'privacy tort') as a matter of urgency.

---

[1] Electronic Frontiers Australia, "Metadata Access for Civil Cases", https://www.efa.org.au/privacy/metadata-civil/ accessed 25 January 2017.

3. Breach of human rights and of TIA aims indicates lack of proportionality and departure from original justifications for Mandatory Data Retention

3.1 ALHR's primary concern is that legislation should adhere to international human rights law and standards. Privacy is a fundamental human right recognized in the UN *Declaration of Human Rights*[2], the *International Covenant on Civil and Political Rights* and in many other international and regional treaties. "Privacy," comments one organisation, "underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age."[3]

3.2 We endorse the views of the Parliamentary Joint Committee on Human Rights (PJCHR) expressed in Guidance Note 1 of December 2014[4] as to the nature of Australia's human, civil and political rights obligations, and agree that the inclusion of human rights 'safeguards' in Commonwealth legislation is directly relevant to Australia's compliance with those obligations.

3.3 We are concerned that relevant legislation relating to access to data retained under the TIA Act should represent **an appropriate and proportionate response to the harms identified by the government as requiring the mandatory retention of data (basically, anti-terrorism security concerns),** and should be consistent with the aims of the TIA Act.

3.4 As the PJCHR states, the aims of the TIA Act are to protect the **privacy of telecommunications**, and to provide a framework for law enforcement and security bodies to apply for warrants to intercept communications when investigating **serious crimes or national security threats**.[5]

- 3.5 In our view, adherence to international human rights law and standards is also an indicator of proportionality.[6] As mentioned, privacy is a human right. There are many aspects to privacy, and indeed it has been said that "in one sense, all human rights are aspects of the right to privacy."[7] Privacy concepts include:
  - **Information Privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
  - **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches;

---

2 Article 12 states: "No-one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks."

3 Privacy International, *Privacy and Human Rights: an International Survey of Laws and Practice*, available at Global Internet Liberty Campaign < http://gilc.org/privacy/survey/intro.html>, accessed 25 January 2017.

4 Commonwealth of Australia, Parliamentary Joint Committee on Human Rights, *Guidance Note 1*: *Drafting Statements of Compatability*, December 2014, available at <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Guidance_Notes_and_Resources> accessed 16 January 2015, see also previous *Practice Note* 1 which was replaced by the Guidance Note, available at< https://www.humanrights.gov.au/parliamentary-joint-committee-human-rights>, accessed 16 January 2015.

5 Commonwealth of Australia, Parliamentary Joint Committee on Human Rights, Fifteenth Report of the 44th Parliament, November 2014, available at <http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Completed_inquiries/2014/Fifteenth_Report_of_the_44th_Parliament>, accessed 16 January 2015.

6 See generally Law Council of Australia, *"Anti-Terrorism Reform Project"* October 2013, <http://www.lawcouncil.asn.au/lawcouncil/images/LCA-PDF/a-z-docs/Oct%202013%20Update%20-%20Anti-Terrorism%20Reform%20Project.pdf> accessed 2 October 2014.

7 Fernando Volio, "Legal personality, privacy and the family" in Henkin (ed) *The International Bill of Rights*, New York, Columbia University Press, 1981, quoted in Privacy International, op cit.

- **Privacy of communications,** which covers the security and privacy of mail, telephones, email and other forms of communication; and
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.[8]

3.6 Unfortunately privacy is not a human right sufficiently protected in Australian law. Nearly every country in the world recognizes a right of privacy explicitly in their Constitution, says Privacy International[9]. But not Australia. While Australia has the Commonwealth *Privacy Act 1988* which contain the *Australian Privacy Principles*, that legislation does not cover all the aspects of privacy mentioned above, and fall far short of providing the protection for Australians' rights needed in relation to the mandatory data retention scheme.

3.7 ALHR opposed the introduction of the mandatory data retention system on a number of grounds including impracticality and lack of requirements around data security. We were particularly concerned that mandatory data retention will **seriously and unreasonably impinge upon the rights of law-abiding Australians** because of the 'indiscriminate, society-wide' invasion of privacy[10] involved. To paraphrase the words of the European Court of Justice:

> '*by requiring the retention of those data and by allowing the competent ... authorities to access those data, the [Bill] interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data*.'[11]

3.8 Neither the sensitivity of the data retained nor the infringement on human rights caused by collection of the data (or by its access) is taken into account under the TIA and unhappily those considerations also seem to be absent from the matters the subject of this Inquiry.

3.9 A fundamental aspect of both privacy of information and of privacy of communication is that material obtained through legal 'surveillance' (such as the mandatory data retention scheme) **must only be used for the purpose for which it was obtained (that is, Australian national security)**. If data which is only retained by telcos and ISPs under the mandatory data retention scheme is to be used in civil litigation, this

(1) breaches the fundamental international privacy principle as to correct use of personal data; and

(2) cannot be justified by the Government's argument that the mandatory data retention scheme is an appropriate and proportionate response to Government security concerns.

Use of such data in civil litigation would include situations where no security issues are involved and where matters are decided only on the balance of probabilities.

3.10 The data retention provisions of the TIA Act **breach Australians' privacy rights and rights to freedom of expression and communication,** contrary to the *International Covenant on Civil and Political Rights* ('ICCPR') to which Australia is a party, and which informs Australian law.

---

8 Privacy International, op cit.

9 op cit.

10 "Write a submission', *Citizens not Suspects*, available at <https://www.citizensnotsuspects.org.au/takeaction/write-a-submission/>, accessed 16 January 2015.

11 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others (8 April 2014), available at http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddaa63d4ce72a047a5a09fe9aa14c2ff0c.e34KaxiLc3qMb40Rch0SaxuPahz0?text=&docid=153045&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=384371, accessed 16 January 2015.

4. Application of International Principles on the Application of Human Rights to Communications Surveillance

4.1 The general principles of data privacy adopted by the US and most European countries include that personal information must be:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date; and
- destroyed after its purpose is completed.[12]

To use data retained under the mandatory data retention scheme for civil litigation would be in breach of these general principles.

4.2 The *International Principles on the Application of Human Rights to Communications Surveillanc*e (IPAHRCS) spell out further how these general principles should be applied to the internet environment. The principles are attached at the end of this document and considered further below.

4.3 We draw your notice in particular to the following principle numbered 11 (emphasis added):

> *INTEGRITY OF COMMUNICATIONS AND SYSTEMS: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Communications Surveillance purposes.* ***A priori data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously****; States should therefore refrain from compelling the identification of users.*[13]

4.4 As you will see from the table below, neither (1) the existing mandatory data retention system itself ('the system'), nor (2) the implicit proposal to access the retained data for civil litigation purposes ('the proposal'), meet the requirements of IPAHRCS.

IPAHRCS principle	Problem
1. Legality	Neither the system not the proposal meet the necessary standards of clarity and precision
2. Legitimate aim	It is not clear what the aim of the proposal is. What is clear however is that it is not the same aim that was the stated justification for the scheme, being security concerns.
3. Necessity and least likely to infringe human rights	These tests are not satisfied.
4. Adequate to achieve aim	The aim of the proposal is not clear therefore the adequacy cannot be assessed. We have argued previously that the scheme is excessive in its scope.
5. Proportionality	This test is not satisfied in relation to either the scheme or the proposal.
6. Competent judicial authority	There are no appropriate protections in relation to the scheme, such as exemptions for journalists or

12 Privacy International, op cit.

13 *International Principles on the Application of Human Rights to Communications Surveillanc*e available at https://en.necessaryandproportionate.org/text#principle_11 accessed 18 January 2015.

IPAHRCS principle	Problem
	whistleblowers (or parliamentarians). In relation to the proposal, legislation by regulation does not involve a competent judicial authority and there is therefore scope for introduction of disproportionate laws.
7. Due process having regard to human rights	This test is not satisfied in either case.
8. User notification	This test is not satisfied in either case.
9. Transparency	This test is not satisfied in either case.
10. Public oversight	This test is not satisfied in either case.
11. Integrity of communications and systems	This test is not satisfied in either case.
12. Safeguards for International Cooperation	Not satisfied in relation to (1). Not relevant to (2)
13. Safeguards against illegitimate access and right to effective remedy	Not satisfied in relation to (1) and not available in relation to (2).

5. Conclusion

5.1 ALHR submits that international law places an obligation upon Australia to:

- protect individual privacy, including the individual's information privacy and communication privacy; and
- justify the legitimacy of any proposed restrictions.

5.2 Any expansion of the existing mandatory data retention system to allow use of retained data in civil litigation is a disproportionate response to the security concerns which were the rationale for the introduction of the system and an unjustified additional encroachment upon Australians' individual privacy. The proposal should not be adopted.

5.3 As we argued in relation to the introduction of the mandatory data retention system, the Government needs to be open and transparent about the principles it will apply in creating and maintaining any Regulations relevant to that system. We are yet to be advised of those principles.

6. ALHR

ALHR was established in 1993 and is a national network of Australian solicitors, barristers, academics, judicial officers and law students who practise and promote international human rights law in Australia. ALHR has active and engaged National, State and Territory committees and a secretariat at La Trobe University Law School in Melbourne. Through advocacy, media engagement, education, networking, research and training, ALHR promotes, practices and protects universally accepted standards of human rights throughout Australia and overseas.

If you would like to discuss any aspect of this submission, please email me at: president@alhr.org.au.

Yours faithfully

Benedict Coyne
President
Australian Lawyers for Human Rights

International Principles on the Application of Human Rights to Communications Surveillance

1	**LEGALITY:** Relevant legislation must meet a standard of clarity and precision sufficient to foresee its application.
2	**LEGITIMATE AIM:** Relevant legislation must: • be intended to achieve (1) a legitimate aim (2) that corresponds to a predominantly important legal interest necessary in a democratic society; and • not be applied in a discriminatory manner.
3	**NECESSITY:** Surveillance laws must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is: • the only means of achieving a legitimate aim, • the means least likely to infringe upon human rights.
4	**ADEQUACY:** Any instance of Communications Surveillance authorised by law must be appropriate to fulfill the specific Legitimate Aim identified.
5	**PROPORTIONALITY:** (1) Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights. (2) Prior to conducting Communications Surveillance, the State must establish the following to a Competent Judicial Authority: • There is a high degree of probability that a serious crime or specific threat to a Legitimate Aim has been or will be carried out, and; • There is a high degree of probability that evidence of a serious crime or specific threat to a legitimate aim would be obtained by accessing the protected information sought, and; • Other less invasive techniques have been exhausted or would be futile and; • Information accessed will be confined to that which is relevant and material; and • Any excess information collected will not be retained, but destroyed or returned; and • Information will be accessed only by the specified authority and used only for the approved purpose; and • That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or fundamental freedoms.
6	**COMPETENT JUDICIAL AUTHORITY:** Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent which is: 1. Separate and independent from the authorities conducting Communications Surveillance; 2. Knowledgeable of issues surrounding the legality of Communications Surveillance, the technologies used and human rights implications; and has adequate resources.
7	**DUE PROCESS:** Due process requires that States respect and guarantee individuals' human rights by ensuring the procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.
8	**USER NOTIFICATION:** Those under surveillance should be notified with enough time and information to enable them to challenge the decision or seek other remedies. Access to the evidence against them should be made available. Delay in notification is only justified in limited circumstances eg ***1.*** notification would seriously jeopardise the purpose of the Communications Surveillance, ***2.*** an imminent risk of danger to human life; ***3.*** authorisation to delay notification is granted by a Competent Judicial Authority and the party affected is notified as soon as a Competent Judicial Authority determines the risk is lifted. The obligation to give notice rests with the State. However, communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.

9	**TRANSPARENCY:** States should be transparent about the use and scope of Communications Surveillance laws. They should publish information on the specific number of surveillance requests approved and rejected and the specific number of individuals affected. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the relevant laws. States should not interfere with service providers who publish the procedures they apply when complying with State requests for Communications Surveillance.
10	**PUBLIC OVERSIGHT:** States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance with authority: • To access all information about State actions, including, where appropriate, access to secret or classified information • To assess whether the State is making legitimate use of its lawful capabilities; • To evaluate whether the State has been accurately publishing information in accordance with its Transparency obligations • To publish periodic reports • To make public determinations as to the lawfulness of those actions.
11	**INTEGRITY OF COMMUNICATIONS AND SYSTEMS:** In order to ensure the integrity, security and privacy of communications systems, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State Surveillance purposes. Data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously. States should therefore refrain from compelling the identification of users.
12	**SAFEGUARDS FOR INTERNATIONAL COOPERATION:** The mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to Communications Surveillance, the standard with the higher level of protection for individuals is applied. Where states seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for Protected Information to circumvent domestic legal restrictions on Communications Surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.
13	**SAFEGUARDS AGAINST ILLEGITIMATE ACCESS AND RIGHT TO EFFECTIVE REMEDY:** States should enact legislation criminalising **illegal** Communications Surveillance by public or private actors. The law should provide civil and criminal penalties, protections for whistleblowers, and avenues for redress by those affected. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence, as is any evidence derivative of such information. Laws are also needed to ensure that material obtained through **legal** Surveillance is: • Only used for the purpose for which it was obtained, and • The material must not be retained, but destroyed or returned to those affected.