



AUSTRALIAN
LAWYERS
FOR
HUMAN RIGHTS

19 January 2015

PO Box A147
Sydney South
NSW 1235
DX 585 Sydney

alhr@alhr.org.au
www.alhr.org.au

The Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra
ACT 2600

By email: dataretention@aph.gov.au

Dear Committee Secretary

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

Australian Lawyers for Human Rights (ALHR) is pleased to provide this submission in relation to the Committee's terms of reference, which are to consider the provisions of the Bill.

As requested, ALHR previously emailed the Committee to confirm that we would be making a submission.

ALHR was established in 1993. ALHR is a network of Australian law students and lawyers active in practising and promoting awareness of international human rights. ALHR has a national membership of over 2,600 people, with active National, State and Territory committees. Through training, information, submissions and networking, ALHR promotes the practice of human rights law in Australia. ALHR has extensive experience and expertise in the principles and practice of international law, and human rights law in Australia.

1. Background

1.1 ALHR's primary concerns are that the Bill (1) should not on its face breach the human, civil or political rights of persons affected by that legislation; and (2) should not be capable of being applied so as to infringe those persons' rights. As the Committee noted in 2013:

*a mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed.*¹

¹ Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Report of Inquiry into Potential Reforms of Australia's National Security Legislation*, June 2013, available at http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm, accessed 18 January 2015, 7, par 1.35.

- 1.2 We endorse the views of the Parliamentary Joint Committee on Human Rights (PJCHR) expressed in Guidance Note 1 of December 2014² 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.
- 1.3 We are concerned that the Bill should represent an appropriate and proportionate response to the harms identified, in the light of the aims of the *Telecommunications (Interception and Access) Act 1979 (TIA Act)*. As the PJCHR states, those aims 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.³ In our view, adherence to international human rights law and standards is also an indicator of proportionality.⁴
- 1.4 We note that the manner in which we legislatively respond to identified concerns is in itself a measure of the strength and nature of our society. As noted by the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism in their *2010 Report*:

*Compliance with human rights while countering terrorism represents a best practice because not only is this a legal obligation of States, but it is also an indispensable part of a successful medium and long-term strategy to combat terrorism.*⁵

2. Main Concerns

- 2.1 We are concerned that the Bill fails both in both practical and legal terms.
- The Bill will not restrict terrorists who wish to avoid its impact and is likely to be readily avoided by Australians generally⁶.
 - It will unreasonably impose enormous costs upon Australians and their internet service providers.
 - It does not impose any absolute requirement upon providers to keep the information secure, and nor do the Australian Privacy Principles⁷.

² Commonwealth of Australia, Parliamentary Joint Committee on Human Rights, *Guidance Note 1: Drafting Statements of Compatibility*, 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.

³ 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.

⁴ 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.

⁵ Quoted in Australian Lawyers for Human Rights, *Submission to the Independent National Security Legislation Monitor*, 25 September 2012, par 8.

⁶ The Communications Alliance/AMTA Submission to this Inquiry states (Section 10, page 16) that there are over 260 secure messaging applications available on the Apple Store which are 'potentially able to remove the user from the reach of the proposed data retention regime.'

⁷ Australian Privacy Principle 11 requires a party to which the Privacy Principles apply and who holds personal information about another only to take 'such steps as are reasonable in the circumstances' to protect the information from misuse, interference, loss, unauthorised access, modification or

- But most of all, it will **seriously and unreasonably impinge upon the rights of law-abiding Australians**. It amounts to an ‘indiscriminate, society-wide’ invasion of privacy⁸ which rebuts the presumption of innocence. It chills freedom of expression and of assembly. It assumes that every Australian is potentially ‘guilty’ and should be monitored. These consequences would be more akin to a police state.⁹
- 2.2 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.*’¹⁰
- 2.3 Both in its current form and its potential operation, the Bill **breaches 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. **It also potentially chills freedom of association.**
- 2.4 How the ICCPR principles should be applied to the internet environment is spelt out further in the *International Principles on the Application of Human Rights to Communications Surveillance* considered at the end of this document. We draw the Committee’s notice in particular to the following principle (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.’¹¹*

- 2.5 ALHR submits that international law places an obligation on Australia to:
- protect individual privacy; and
 - justify the legitimacy of any proposed restrictions on freedom of speech and communication.

The current wording of the Bill is so broad that it both breaches the International Principles and **places Australia in breach of its obligations under the ICCPR**. There is no

disclosure. There are numerous areas in which the Privacy Principles will not fit well with the Bill and will need to be modified.

⁸ “Write a submission”, *Citizens not Suspects*, available at <https://www.citizensnotsuspects.org.au/takeaction/write-a-submission/>, accessed 16 January 2015.

⁹ See submission from Office of the Victorian Privacy Commissioner, Submissions received to the Inquiry into potential reforms of National Security Legislation Reforms, no 109, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm, accessed 16 January 2015.

¹⁰ 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.

¹¹ *International Principles on the Application of Human Rights to Communications Surveillance* available at https://en.necessaryandproportionate.org/text#principle_11 accessed 18 January 2015.

established need for blanket data retention (and therefore potential ‘fishing expedition’ monitoring) of every man, woman and child in Australia.

- 2.6 Contrary to recent statements,¹² there is absolutely **no urgency for this Bill to be passed** and in fact ALHR believes that Australians would be better off if it were abandoned. The urgent passing of this Bill will cause more problems than it solves. The Bill should be subject to full and considered public and Parliamentary scrutiny, particularly in the light of the concerns expressed already by PJCHR and the Senate Standing Committee for the Scrutiny of Bills.
- 2.7 More appropriate and proportionate powers already exist which enable law enforcement and intelligence agencies to issue ‘Data Preservation Notices’ that compel ISPs to retain all information about persons of interest (including the content of communications) for a fixed period.¹³
- 2.8 We endorse the submissions of the Gilbert and Tobin Centre and of the Law Institute of Victoria, and the position of the Law Council of Australia¹⁴, in relation to these issues.

3. Comparisons

Human Rights

- 3.1 The Explanatory Memorandum acknowledges (p 10, par 29) that the Bill ‘engages’ the following rights:
- protection against arbitrary or unlawful interference with privacy (Article 17, ICCPR);
 - the right to a fair trial, the right to minimum guarantees in criminal proceedings and the presumption of innocence (Article 14, ICCPR);
 - protection of the right to freedom of expression (Article 19, ICCPR and of the Universal Declaration of Human Rights). This includes, according to the ICCPR, ‘freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print ... or through any other media of his choice.’¹⁵
- 3.2 ALHR submits that the Bill also negatively impacts upon:
- the right to be treated with dignity (Article 1, Universal Declaration of Human Rights);
 - freedom from arbitrary interference with privacy, family, home **or correspondence** (Article 12, Universal Declaration of Human Rights);
- and is likely to chill:

¹² Daniel Hurst, ‘Data retention bill an ‘urgent priority’ to counter terrorism, George Brandis says,’ *The Guardian*, 12 January 2015, available at: <<http://www.theguardian.com/australia-news/2015/jan/12/data-retention-bill-an-urgent-priority-to-counter-terrorism-george-brandis-says>>, accessed 16 January 2015.

¹³ See Section 107G of the TIA Act and iiNet’s comments in the context of the Senate Committee inquiry into the reform of the TIA Act, available at <<http://www.iinet.net.au/about/mediacentre/papers-and-presentations/iinets-response-to-questions-on-notice.pdf>> accessed 16 January 2015.

¹⁴ See Law Council of Australia, “Law Council of Australia does not support mandatory data retention proposal”, Media Release #1429, 3 December 2014, <http://www.lawcouncil.asn.au/lawcouncil/images/LCA-PDF/mediaReleases/1429_-_Law_Council_of_Australia_does_not_support_mandatory_data_retention_proposal.pdf>, accessed 16 January 2015.

¹⁵ It also argues (p 29, par 135ff) that the Bill, by enabling Australian-wide surveillance of telecommunications data, indirectly protects Australians and hence engages the right to life (Articles 6 of the ICCPR) and the right to security of the person (Article 9 of the ICCPR).

- freedom of association (Articles 21 and 22, ICCPR and Article 20, Universal Declaration of Human Rights);
- the right to free development of one's personality (Article 22, Universal Declaration of Human Rights);
- the right to take part in the conduct of public affairs (Article 25, ICCPR)¹⁶;
- press freedoms.

Standards in Comparable Jurisdictions

3.3 As noted in the 'Statement of Compatibility' in the Explanatory Memorandum (par 66 ff), in 2014 the European Court viewed similar legislation as NOT proportionate to the perceived harm to be addressed because:

- a) it covered, in a generalised manner, all individuals, all means of electronic communication and all traffic data **without any differentiation**, limitation or exception being made in the light of the objective of fighting against serious crime (the Bill also fails here; see PJCHR pars 1.31 and 1.52 where PJCHR notes that the Bill fails to take account of additional privacy issues such as legal professional privilege or journalists' concern to protect their sources (PJCHR par 1.70). Nor are there any exemptions for data that shows 'communications' by or with doctors, priests or politicians);
- b) it failed to lay down any objective criterion which would ensure that authorities are allowed to access the data and **use it only for the purposes of** prevention or detection of serious criminal offences (the Bill also fails here; see PJCHR par 1.48);
- c) access to the data was not made dependent on the **prior review by a court** (the Bill also fails here; see PJCHR par 1.57 ff);
- d) the data retention period was arbitrary and **not limited to what is reasonably necessary** in relation to the objective pursued and the legislation failed to make any distinction between the **categories of data** on the basis of the persons concerned or the possible usefulness of the data (the Bill also fails here; see PJCHR par 1.40ff and Communications Alliance/AMTA Submission, Attachment 1, page 20);
- e) the legislation did not provide for sufficient safeguards to ensure effective protection of the data by ISP providers against the **risk of abuse** and against any unlawful access and use of the data and did not ensure the **irreversible destruction** of the data at the end of the retention period. Nor did it require the data to be retained in the relevant jurisdiction. (The Bill has no requirements for safeguarding of data by ISP providers or by government bodies. It has no requirements itself for destruction of data by ISP providers and it is unclear whether metadata would be covered by the existing requirements for document destruction in the TIA Act. In addition, PJCHR has expressed concerns about what would happen to data shared within Australia

¹⁶ 'Absent such a freedom of communication' said Mason CJ, 'representative government would fail to achieve its purpose, namely, government by the people through their elected representatives; government would cease to be responsive to the needs and wishes of the people and, in that sense, would cease to be truly representative... The efficacy of representative government depends also upon free communication on such matters between all persons, groups and other bodies in the community.' *Australian Capital Television Pty Ltd & New South Wales v Commonwealth* [1992] HCA 45; (1992) 177 CLR 106 (30 September 1992) [38 -39].

between government agencies: PJCHR par 1.50). There is also the issue of the sharing of data with other countries.¹⁷

4. Practical Problems

- 4.1 Our understanding from the comments made by a number of other parties including service providers is that the Bill does not establish a practically workable regime.
- 4.2 The Bill 'outsources' compliance to private companies. This arrangement unfairly imposes an enormous cost which will be passed on to consumers, will have anti-competitive results as it is likely to drive smaller operators out of business and unfairly penalises companies with eligible infrastructure in Australia as against overseas companies.¹⁸ It is not a 'level playing field'.
- 4.3 All of the above are undesirable results from a free market point of view.
- 4.4 Operators (no matter how large) may not be able to keep the relevant data confidential and secure from local or foreign hackers. There is a **substantial risk of abuse** in the system required under the Bill.
- 4.5 We will not expand on these issues which are better described by others more expert in these areas. We endorse the submission of Communications Alliance/Australian Mobile Telecommunications Association in relation to these issues.

5. Legal Problems

Lack of Certainty

- 5.1 The relevant data set to be retained is not yet determined (s 187A(1) although the general outlines are contained in s 187A(2)) and remains to be decided by Regulation. This is **bad legislative practice and likely to result in legislative 'creep'** with individuals' privacy rights being increasingly attacked through expansion of the data set, as noted by a number of commentators including the PJCHR and the Senate Standing Committee for the Scrutiny of Bills¹⁹ ('Senate Committee').
- 5.2 The retention period can be extended by Regulation (s 187C(2)) which arouses the same concerns as to the possibility of regulatory 'creep'.
- 5.3 Although s187 states that content must not be collected, content is not defined and aspects of the data which is apparently intended to be retained overlap with content information (see PJCHR par 1.38).²⁰
- 5.4 Proposed subsection 110A(3) empowers the minister to declare, by legislative instrument, further authorities or bodies to be a 'criminal enforcement agency' thereby enabling agencies beyond those listed in subsection 110A(1) to access metadata under the TIA Act. Proposed subsection 176A(3) similarly empowers the minister to expand the meaning of 'enforcement agency'. ALHR agrees with the Senate Committee that this amounts to an inappropriate delegation of legislative power. Although the Bill requires the Minister to take certain factors into account in making these declarations, the enumerated factors are

¹⁷ Don Reisinger, 'UK to seek Obama's help in accessing user data from US firms', CNET, available at <http://www.cnet.com/news/uk-to-seek-obamas-help-in-accessing-user-data-from-us-firms/>, 15 January 2015, accessed 16 January 2015.

¹⁸ Communications Alliance/AMTA Submission, section 11, 17.

¹⁹ Alert Digest No 16 of 2014, 26 November 2014, 2 ff, available at <http://www.aph.gov.au/~media/Committees/Senate/committee/scrutiny/alerts/2014/pdf/d16.pdf> accessed on 16 January 2015.

²⁰ PJCHR, *Fifteenth Report on 44th Parliament*, op cit.

not determinative. ALHR agrees with the Senate Committee that further safeguards in this area requiring Parliamentary approval and oversight are required.

Overreach

5.5 It is arguable rather that the existing definition of metadata in the TIA Act should be restricted because it was drafted many years ago when types and quantities of metadata were quite different²¹ and minimal information could be accessed through communications technologies. Therefore the drafting did not take into account:

- modern technologies and techniques;
- the ability of the State to combine and organize information gained from different surveillance technologies and techniques;
- the increased sensitivity of personal information available to be accessed;
- the necessity for transparency and accountability in this area;
- the way in which modern technologies could impact upon human rights;
- best practice in other countries (in terms of a balance between protection of human rights and law enforcement interests).

Those matters need to be taken into account in the Bill.²²

5.6 As mentioned above in section 3, the Bill is not tailored so as to provide a proportionate response in relation to concerns about specific individuals or classes of individuals, but requires retention of data about everybody within Australia. This is clearly disproportionate to the Bill's aims.

Lack of Transparency means lack of accountability

5.7 The Bill enables authorised entities to access personal metadata **without a warrant**. As the Communications Alliance/AMTA submission to the Inquiry points out, it is ironic that a warrant is required for the content of a communication (which may contain little information) but no warrant is required for a large amount of personal metadata which can build up a much more complete picture about an individual. This result doubtless reflects the fact that with advances in technology there is - to use an unfortunate analogy which has been heavily criticised – now effectively more information on the outside of 'the envelope' than inside it²³. Today, warrants should be required to access metadata so that (1) individuals may not be investigated by government bodies without proper cause, and so that (2) an appropriate check or balance is applied through the mechanism by which the warrant is obtained from the courts.

To remove the requirement for prior authorisation via a warrant is to undermine both democracy and the rule of law by reducing the checks and balances essential to a democratic system.²⁴ (See also Section 6 below into the changes that have occurred to transparency under Australian legislation).

5.8 Australians will not know what information about them has been obtained, nor by whom. ALHR endorses the suggestion of the PJCHR that at the very least, there should be a

²¹ PJCHR, *Fifteenth Report on 44th Parliament*, op cit, par 1.22.

²² See generally PJCHR, *Fifteenth Report on 44th Parliament*, op cit, par 1.47.

²³ David Glance, "What politicians say about Metadata: Bad metaphors and a bad idea", *The Conversation*, 7 August 2014, available at <http://theconversation.com/what-politicians-say-about-metadata-bad-metaphors-and-a-bad-idea-30247>, accessed 16 January 2014. The Explanatory Memorandum notes at 7, par 13 that: 'The availability of encrypted services is also impacting on the utility of access to telecommunications content, making telecommunications data an increasingly valuable investigative tool.'

²⁴ Sections 8, 13.

requirement for delayed notification to an individual that their data had been subject to an application for an authorisation for access and appropriate provisions to allow individuals to challenge such access (PJCHR par 1.73ff).

Lack of Safeguards chills free speech/ expression/ communication, freedom of association

- 5.9 The fact that the content of the data will not be retained is irrelevant to the Bill's impingement upon privacy rights. Users will still be able to be identified and **significant information about them will be obtainable**.²⁵ The Bill will have a 'chilling' effect upon the **act of free speech** as Australians will not know what information about them, including information about their contacts, might be shared amongst government (and perhaps even non-government) bodies. This is acknowledged by the Statement of Compatibility with Human Rights.²⁶

As Professor Arnold says: *We should not be subject to the chill associated with knowing that the police – and other entities – will be able to identify who we called, who read our tweets, when we called, where we were located, whether we visited Facebook and who read our posts. The data should not be provided without a warrant.*²⁷

As the UN Human Rights Committee has noted, the rights to information and to freedom of expression are integral to **freedom of association** as expressed in group advocacy, political organizing, vindication of rights, civil society monitoring, and many other associative activities in a normal democratic society.²⁸

Impact on Press Freedom

- 5.10 A joint Human Rights Watch and American Civil Liberties Union report in July 2014²⁹ documented 'the insidious effects of large-scale [digital] surveillance on journalism and law in the United States.' Interviews with dozens of leading journalists showed that increased surveillance is stifling reporting and hence limiting the ability of the media to act as a check on governmental wrongdoing.

*Many journalists said it is taking them significantly longer to gather information (when they can get it at all), and they are ultimately able to publish fewer stories for public consumption. ... these effects stand out most starkly in the case of reporting on the intelligence community, national security, and law enforcement—all areas of legitimate—indeed, extremely important—public concern.*³⁰

- 5.11 This effect damages the role of the fourth estate, notes Human Rights Watch, and restricts the amount of information available to citizens, particularly on matters of public concern related to national security.³¹ In this way, 'effective democratic participation and governance' is undermined.³²

²⁵ To quote the European Court: 'Those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.'

²⁶ Explanatory memorandum, 5 and 28, par 129ff and see also PJCHR, *op cit*, par 1.68ff.

²⁸ UN Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, U.N. Doc. CCPR/C/GC/34 (2011), para. 4, and see Human Rights Watch and Civil Liberties Union, *With Liberty to Monitor All*, 2014, accessed 17 January 2015, available at http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUpload_0.pdf, 80.

²⁹ Human Rights Watch and Civil Liberties Union, *op cit*.

³⁰ Human Rights Watch and Civil Liberties Union, *op cit*, 4.

³¹ Cynthia Wong, Human Rights Watch, "Reclaiming Privacy in the Age of Surveillance", Common Dreams, 13 January 2015, available at

Impact on Legal Professional Privilege

- 5.12 The ICCPR has been interpreted as protecting the full confidentiality of communications between client and lawyer. The Bill does not, however, permit any exemptions for lawyer/client communications. The mere fact that the government acquires and retains materials about such communications, even if they are never used, conflicts with lawyers' ethical obligations to keep that information confidential.³³

Lack of safeguards for accessed metadata

- 5.13 **The Bill would appear to contain no safeguards about what happens to the data once it is accessed.** The data might only be kept by the service provider for two years, but once it is accessed by an authority it would appear that – unless Australian Privacy Principles apply – it can be kept forever.

6. Conclusion

- 6.1 ALHR acknowledges that it is vital to achieve a proportionate and effective balance between the government's domestic and international obligations to protect its citizens from terrorism and serious crimes, and its international obligations to preserve and promote its citizens' fundamental human rights.
- 6.2 However it is also essential that security laws adhere to the Australian government's international legal obligations under various binding instruments and accord with agreed norms of human rights, civil liberties and fundamental democratic freedoms. If legislative provisions do not accord with these standards they should not be adopted.
- 6.3 ALHR believes that a human rights framework will strengthen counter-terrorism and national security laws in Australia by appropriately balancing the various obligations. This Bill does not reflect an appropriate balance.

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

Yours faithfully



Nathan Kennedy

President
Australian Lawyers for Human Rights

Contributors: Dr Tamsin Clarke, Vicki Lambert, Mila Dragicevic, Socrates Aronis, David Rofe, Soung Takayama

<<http://www.commondreams.org/views/2015/01/13/reclaiming-privacy-golden-age-surveillance?utm>>, accessed 17 January 2015.

³² Human Rights Watch and Civil Liberties Union, *op cit*, 44.

³³ Human Rights Watch and Civil Liberties Union, *op cit*, 51, 91.

Does the Bill meet the International Principles on the Application of Human Rights to Communications Surveillance?

	International Principle (summarised)	<i>Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014</i>
1	<p>LEGALITY: Relevant legislation must meet a standard of clarity and precision sufficient to foresee its application.</p>	<p>Information which may be accessed remains to be defined by Regulation (s 187A) which is highly undesirable. Foreseeability is linked to transparency and at the very least the principles guiding the creation and maintenance of any Regulations should be made available to this end. Many other aspects can also be varied by Regulation (see pars 5.1 – 5.4 in the body of the Submission).</p>
2	<p>LEGITIMATE AIM: Relevant legislation must:</p> <ul style="list-style-type: none"> • 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. 	<p>The Bill is too broadly drafted and in its effect will depart from the aims of the original Act (see par 1.3). Freedom of expression is arguably an interest that is more necessary in a democratic society than the government’s interest in collecting personal data about all Australians for potential surveillance purposes.</p>
3	<p>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:</p> <ul style="list-style-type: none"> • the only means of achieving a legitimate aim, • the means least likely to infringe upon human rights. 	<p>Legislation requiring the retention of specific information about every Australian for potential surveillance purposes is not strictly and demonstrably necessary. Such measures should apply only to persons of concern and be subject to a warrant.</p>
4	<p>ADEQUACY: Any instance of Communications Surveillance authorised by law must be appropriate to fulfill the specific Legitimate Aim identified.</p>	<p>There is no transparency in the Bill around this issue because no warrant is required for various authorities to access personal data.</p>
5	<p>PROPORTIONALITY: (1) Decisions about Communications Surveillance must consider the sensitivity of the information accessed and the severity of the infringement on human rights.</p> <p>(2) Prior to conducting Communications Surveillance, the State must establish the following to a Competent Judicial Authority:</p> <ul style="list-style-type: none"> • 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 	<p>(1) Under the Bill neither the sensitivity of the information nor the infringement on human rights caused by collection of the information (or by its access) is taken into account.</p> <p>(2) There is no requirement for any government authority to prove each of these points or meet these targets before proceeding with accessing personal metadata.</p> <p>If it can be demonstrated that obtaining all Australians’ metadata is necessary and appropriate (which is in question), as well as being effective in achieving its objective, then the interference with human rights must still be proportionate to the risk posed by the relevant criminal activity in question.</p>

	International Principle (summarised)	<i>Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014</i>
	<ul style="list-style-type: none"> That the surveillance activities requested and techniques proposed do not undermine the essence of the right to privacy or fundamental freedoms. 	
6	<p>COMPETENT JUDICIAL AUTHORITY: Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent which is:</p> <ol style="list-style-type: none"> Separate and independent from the authorities conducting Communications Surveillance; Knowledgeable of issues surrounding the legality of Communications Surveillance, the technologies used and human rights implications; and <p>has adequate resources.</p>	<p>The Bill does not allow for judicial consent to be obtained <u>before</u> metadata is collected or before it is obtained by authorised agencies for surveillance purposes.</p>
7	<p>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.</p>	<p>Following the right to procedural fairness, an affected individual should be afforded the right to present their case before their metadata is accessed. The Bill makes no provision for this. Nor are the procedures according to which the Bill is applied made public.</p>
8	<p>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.</p> <p>Delay in notification is only justified in limited circumstances e.g.</p> <ol style="list-style-type: none"> notification would seriously jeopardise the purpose of the Communications Surveillance, an imminent risk of danger to human life; 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. <p>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.</p>	<p>There are no equivalent provisions under the Bill. Central to our judicial system is the principle of a fair hearing. This applies when an administrative decision affects a person's rights, interests or legitimate expectations in a direct and immediate way³⁴. Here an individual's interest in freedom of communication is affected and thus judicial review of any access by authorised authorities to personal data is appropriate.</p>
9	<p>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</p>	<p>The Bill has no such requirements and it is not government practice to provide such information.</p>

34

Kioa v West (1985) 159 CLR 550 [584]

	International Principle (summarised)	<i>Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014</i>
	should not interfere with service providers who publish the procedures they apply when complying with State requests for Communications Surveillance.	
10	<p>PUBLIC OVERSIGHT: States should establish independent oversight mechanisms to ensure transparency and accountability of Communications Surveillance with authority:</p> <ul style="list-style-type: none"> • 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. 	No such mechanisms appear to exist in relation to the Bill
11	<p>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.</p> <p>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.</p>	The Bill clearly breaches this provision.
12	<p>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.</p> <p>Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.</p>	The Bill has no such requirements.
13	<p>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.</p> <p>Laws are also needed to ensure that material obtained through legal Surveillance is:</p>	<p>The Bill has no such requirements.</p> <p>There is undeniable potential for abuse. With no specific penalties to complement an abuse of the power under the Bill, the Bill's reach is disproportionate.</p>

	International Principle (summarised)	<i>Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014</i>
	<ul style="list-style-type: none">• Only used for the purpose for which it was obtained, and• The material must not be retained, but destroyed or returned to those affected.	