AUSTRALIAN LAWYERS FOR HUMAN RIGHTS

10 September 2018

PO Box A147
Sydney South
NSW 1235
DX 585 Sydney

www.alhr.org.au

Minister for Home Affairs
Parliament House
Canberra ACT 2600

By email: assistancebill.consultation@homeaffairs.gov.au

Dear Minister

Consultation in relation to the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*

Australian Lawyers for Human Rights (**ALHR**) appreciates the opportunity to provide this submission. Given the length of the Bill and the timeframe for submissions, it should be noted that this submission is not exhaustive and that other problems may exist with the Bill which are not covered here.

1. ALHR's Concerns

1.1 Pursuant to the principle of legality, Australian legislation should adhere to international human rights law and standards, unless legislation contains clear and unambiguous language otherwise. Furthermore, the Australian parliament should properly abide by its binding obligations to the international community in accordance with the seven core international human rights treaties and conventions that it has signed and ratified, according to the principle of good faith.

1.2 ALHR endorses the views of the Parliamentary Joint Committee on Human Rights (PJCHR) expressed in Guidance Note 1 of December 2014[1] 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 It is only through holding all behaviours up to the standard of international human rights that one can help improve and reform harmful and discriminatory practices.

---

[1] 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>, 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>.

1.4 Legislation should represent an **appropriate and proportionate response** to the problems and issues addressed by that legislation, and adherence to international human rights law and standards is an important indicator of such proportionality.[2]

1.5 We are concerned that the Bill should represent **an appropriate and proportionate response to the harms identified by the government,** and should be consistent with the aims of the *Telecommunications Act* and the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Our concern is that such is not the case.

1.6 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**.[3]

1.7 Privacy is a fundamental human right recognized in the UN *Declaration of Human Rights*[4], the *International Covenant on Civil and Political Rights* (ICCPR) 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."[5]

1.8 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."[6] Privacy concepts include **Privacy of communications,** which covers the security and privacy of mail, telephones, email and other forms of communication.

1.9 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[7]. 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 proposed Bill.

1.10 ALHR is particularly concerned that the Bill will **seriously and unreasonably impinge upon the rights of law-abiding Australians** because of the indiscriminate invasion of privacy which could be involved. To paraphrase the words of the European Court of Justice:

> '*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*.'[8]

---

2 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> .

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>

4 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."

5 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>.

6 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.

7 op cit.

8 Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others (8 April 2014), available at

1.11 The Bill **breaches Australians' privacy rights and rights to freedom of expression and communication,** contrary to the ICCPR to which Australia is a party, and which informs Australian law. Arguably the Bill also limits the presumption of innocence by allowing covert access to personal communications and criminalising the refusal to share one's passwords.

1.12 Australia is a contracting party to the ICCPR which was signed by the Australian government on 18 December 1972 and ratified on 13 August 1980. Pursuant to Article 26 of the 1969 Vienna Convention on the Law of Treaties, Australia is obliged to the international community to implement, uphold, protect and respect all of the rights contained in the ICCPR including the right to freedom of expression and the right to a fair and public hearing in both civil and criminal proceedings.

1.13 ALHR opposes the provisions of the Bill which are inconsistent with the principles that form the bedrock of Australia's criminal justice system as well as international human rights standards.

2. Summary of Problems with the Bill

Australia, which has no bill of rights, is a logical place to test new strategies for collecting intelligence that can later be adopted elsewhere.[9]

2.1 This Bill goes against worldwide best practice in digital privacy

In the same year that Europe has introduced the General Data Protection Regulation in the interests of protecting the digital privacy of European citizens, Australia is proposing legislation that would allow covert installation by government of programmes that are effectively malware into Australians' computers and phones and would penalise people who refuse to give the government their passwords[10] with imprisonment for 10 years or 600 penalty units (being over $120,000) or both - irrespective of whether or not any harm was involved. The contrast between concern for citizens' rights in Europe – and lack thereof in Australia - could not be starker.

Australians should be able to have privacy, security and integrity for our communications and our communications systems. No legislation, executive order, or private agreement between systems providers and the government should undermine digital privacy rights in a manner that is not appropriate or proportionate to the harm sought to be addressed and without adequate transparency and oversight.

The Australian government should not erode *en masse* the security of our devices or applications, pressure companies to keep and allow government access to our data, mandate implementation of vulnerabilities or backdoors into products, or have disproportionate access to the keys to private data.

2.2 This Bill is impractical and could have serious cybersecurity and economic effects

This Bill has international implications: it breaches key privacy rights not only for Australians but for all customers of affected companies (no matter where they may be in the world. The Bill allows the Director-General of Security or the chief officer of an interception agency to compel a provider

---

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.

9 Lizzie O'Shea, Australia Wants to take Government Surveillance to the next Level", *New York Times* online 4 September 2018 at https://www.nytimes.com/2018/09/04/opinion/australia-encryption-surveillance-bill.html

10 See definition of 'access' in section 317B.

(telco/isp) to do an unlimited range of *acts or things*, which could mean anything from removing security measures to deleting messages or collecting extra data. Providers will also be required to conceal any action taken covertly by law enforcement.

Further, the Attorney General may issue a "technical capability notice" *directed towards ensuring that the provider is capable of giving certain types of help* to ASIO or an interception agency. Effectively it appears that companies may be required to provide confidential and sensitive information about how their systems work, and to assist the government in bypassing those companies' security (particularly encryption) systems, if that is possible. The range of services providers covered would appear to include telecommunication companies, internet service providers, email providers, social media platforms and a range of other "over the top" services (any app or service that provides a product over the Internet and bypasses traditional distribution) as well as those who develop, supply or update software, and who manufacture, supply, install or maintain data processing devices.

In addition to the serious human rights concerns that such broadly drafted and wide ranging measures give rise to, ALHR submits that the provisions are impractical. Major international corporations are extremely unlikely to meet the requirements that the Australian government might seek to impose upon them under the Bill, if it is enacted. It is not clear how the companies which are asked to assist the Australian government in such matters are expected to fund the work they are required to do nor how they are expected to cope with the consequential reputational damage, should their assistance in undermining their own systems become known.

If carried into effect, the measures would enormously increase the likelihood of new and uncontrollable computer threats and vulnerabilities worldwide through its proposed use against encryption. Weakening encryption weakens the entire Internet and increases risks for everyone on it.

As Access Now comments: '*encryption protocols are the backbone of the digital economy, facilitating every single transaction online.*' The Bill appears to be aimed at reducing the security of encryption systems worldwide which could have disastrous and unforeseen effects internationally on both industry and governments. While we are not experts in this area (and so refer the Department to the concerns expressed by many peak technological organisations), it is clear that the international implications of this Bill are of serious concern.

It would seem that, by disproportionately impinging upon everyone's right to privacy, what the Bill is most likely to do is to drive criminal communications further underground, encouraging criminals to use devices that cannot be intercepted, while at the same time weakening or imperilling valid encryption methods used legitimately for world wide commerce and banking.

2.3 Government activities under the Bill might breach 'national security'

The Bill refers throughout to the interests of Australia's 'national security,' 'foreign relations' and 'national economic well-being' as providing justification for the various types of activities which the government might undertake under the Bill.

Ironically, as indicated above, all these interests are more likely to be impacted in a negative manner should the government put into effect the powers proposed under the Bill. Indeed, given that the recently expanded definition of 'national security' in section 90.4 of the Criminal Code now includes Australia's economic relations with other countries, we query whether government agency actions pursuant to the Bill, should it become law, might actually involve breaches of Australia's own national security. Government departments will not be immune from the very system weaknesses that the Bill seeks to create.

2.4 This Bill gives government inappropriate powers without adequate checks and balances

This Bill grants government officials power to both compel organisations to reveal information about their systems and to make changes to those systems. Combined with the proposed new ability for government to issue warrants to seize information directly from devices, this would effectively empower Australian government agencies to become 'legal' hackers with minimal legislative restrictions or oversight mechanisms. As O'Shea says:

> *If we give state agencies more power to build tools to circumvent encryption, not only do we expose ourselves to the risk that they can be stolen, we are forced to trust that these agencies will behave responsibly. The evidence to date suggests the opposite.*
>
> *Worse still, the Australian government hardly has the best reputation for keeping things safe.*

We note that the Bill appears to be based upon similar English legislation but without the specific judicial oversight regime established under that legislation, which includes an Investigatory Powers Commissioner. We submit that a judicial oversight regime is essential here too.

3. Human rights breached by the proposed Bill

3.1 The Explanatory Memorandum fails to identify any rights under the *International Covenant on Civil and Political Rights* (**ICCPR**) as potentially impacted, and refers only 9 times in 114 pages to the concept of 'privacy' – generally to say that 'privacy will be protected through robust safeguards.'

3.2 In addition, the Bill continues this government's concerning and very undesirable pattern of criminalising behaviour that is in no way intended to cause harm, and quite irrespective of whether or not harm has actually been caused. Given that (in the name of the very broadly-defined concept of 'national security') the Bill might result in incarceration for non-malignant behaviour which actually causes no harm, the Bill is potentially in breach of Article 9 of the ICCPR and Article 3 of the *Universal Declaration of Human Rights* (**UDHR**) which protect the right to liberty.

3.3 We remind the Committee that Australia had a significant role in drafting the UDHR and in its adoption by the United Nations General Assembly on 10 December 1948. This is a proud history that Australia has in upholding basic human rights and we should be vigilant to guard against their infringement by the government of the day.

3.4 We note also that Australia campaigned for its seat on the United Nations Human Rights Council on that basis that it is an 'international human rights leader' with 'respect for democracy and the rule of law.'

3.5 Finally we note that, in stark contrast to citizens in comparable democracies across the Western world, Australians do not enjoy the domestic protection of their human rights due to the absence of any federal Human Rights Act.

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.[11]

These general principles are not respected in the Bill.

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 current digital 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.*[12]

IPAHRCS principle	Problem
1. Legality	The powers under the Bill do not meet the necessary standards of clarity and precision
2. Legitimate aim	While the aim of gathering information relating to local Australian criminal behavior may be legitimate, the manner in which this is proposed to be achieved, being by the introduction of uncontrollable software equivalent to 'malware' and the weakening of encryption which could have worldwide impact, is so disproportionate as to render the aim illegitimate.
3. Necessity and least likely to infringe human rights	These tests are not satisfied.
4. Adequate to achieve aim	The Bill is excessive in its scope.
5. Proportionality	This test is not satisfied.
6. Competent judicial authority	There are no appropriate protections in relation to the proposed government powers.
7. Due process having regard to human rights	This test is not satisfied.
8. User notification	This test is not satisfied.
9. Transparency	This test is not satisfied.
10. Public oversight	This test is not satisfied.
11. Integrity of communications and systems	This test is not satisfied.
12. Safeguards for International Cooperation	This test is not satisfied.
13. Safeguards against illegitimate access and right to effective remedy	This test is not satisfied.

11 Privacy International, op cit.

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

5. Conclusion

5.1 Any legislation which impinges upon human rights must be narrowly framed, proportionate to the relevant harm it addresses, and provide an appropriate contextual response which minimises the overall impact upon all human rights. ALHR is concerned that in significant respects the Bill does not strike the right balance.

5.2 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.

5.3 The Bill is a disproportionate response to the security concerns which are its rationale, involving unjustified encroachments upon Australians' individual privacy and potentially disastrous world-wide consequences for communications security. As O'Shea says:

> *The Australian government is testing the limits of our democracy by seeking to empower the surveillance state, and what it learns will have implications globally. We need to take a stand against this power grab by state agencies, and reject the idea that encrypted communications undermine security. Quite the opposite …*

ALHR is happy to provide any further information or clarification in relation to the above if government so requires.

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

Yours faithfully

Kerry Weste

President

Australian Lawyers for Human Rights

ALHR

ALHR was established in 1993 and is a national association 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 specialist thematic committees. Through advocacy, media engagement, education, networking, research and training, ALHR promotes, practices and protects universally accepted standards of human rights throughout Australia and overseas.

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.