Australian Privacy Foundation

https://www.privacy.org.au

Secretary@privacy.org.au

https://privacy.org.au/about/contacts/

4 June, 2019

INTERNATIONAL IMPLICATIONS OF THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018

Introduction

This report, prepared by the Australian Privacy Foundation,[1] analyses the international ramifications of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) ('AA Act'), which amends the *Telecommunications Act 1997* ('TA'). It evaluates the legal obligations that could be imposed upon "designated communication providers"[2] offering services or systems that are accessible by Australian internet and telecommunications users. It focuses on how service providers located anywhere in the world could be compelled to develop technology to assist Australian security agencies to access encrypted information with very limited oversight. In addition, it reviews how foreign governments may be able to use the legislation for their own investigatory purposes under the purview of a joint investigation with Australia. This paper concludes with a summary of the main issues and concerns regarding the international significance of the legislation.

Executive Summary of Issues

The AA Act has wide implications for the international community as it has been enacted despite:

- Vague and unclear limits on ill defined, wide reaching powers;
- Involving Australia's enforcement of laws of foreign countries including countries with the death penalty or offences not recognised in Australia (lack of dual criminality);
- Limited transparency and a lack of detailed reports accessible to Australians seeking to assess threats impacting on their information security;
- The removal of judicial review; and,

[1] This report has been prepared by Mr Dylan Ford and Dr Monique Mann. We thank Dr Roger Clarke, Dr Chris Culnane, Ms Carly Kind, Mr David Vaile, Dr Ian Warren, Ms Kat Lane, and Professor Lee Bygrave for review.

[2] AA Act s 317C.

- Enhanced capability for information sharing among 'Five Eyes' (intelligence services from Australia, New Zealand, Canada, the UK and the US) nations, with no effective protections from abuse or misuse due to a lack of human rights protections for Australians.

Background and Context

The AA Act was introduced to the Australian Parliament in September 2018 and was passed in December 2018, with pre-election urging about unspecified Christmas season threats apparently suppressing robust review. The Act mandates a dramatic and controversial expansion of law enforcement and intelligence service powers criticised by media, experts in encryption and privacy advocates.[3]

The AA Act creates extraterritorial implications in three ways that raise numerous concerns:

1. Obligations that can be imposed on 'designated communications providers' outside Australia through the issuing of:
    - Technical Assistance Requests, s 317G
    - Technical Assistance Notices, s 317L
    - Technical Capability Notices, s 317T
2. Expansion of Australia's computer access warrants to apply internationally, and to allow for their use in the enforcement of foreign laws (rather than domestic laws).
3. Exploitation of absent human rights protections to engage in further information-sharing with the other nations, including 'Five Eyes' partners under amendments to the *Mutual Assistance in Criminal Matters Act 1987* (Cth).

'Designated Communications Providers'

The legislative scheme of the new TA Part 15, inserted by Schedule 1 of the AA Act, allows the Director-General of Security and intelligence agencies to issue a series of requests and notices to a "designated communications provider".[4] This is a significant change as the executive authorisation of these notices does not require the independent review and approval of a judge.

[3] Peter Knight and Luke Dailey "Draft Home Affairs Bill vastly overreacts its stated purposes and is susceptible to abuse: 'Telecommunications and Other Legislative Amendment (Assistance and Access) Bill 2018' (Cth)" (2018) 15(8) *Privacy Law Bulletin* 134; Monique Mann, 'The devil is in the detail of government bill to enable access to communications data', *The Conversation* (15 August 2018) <https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909>.
[4] *AA Act* (n 2) s317C.

"Designated communications provider" is defined broadly in s 317C to include, inter alia, not only carriers, carriage service providers, related intermediaries and ancillary service providers, but also any provider[5] of an "electronic service"[6] that has one or more end-users in Australia, or of software likely to be used in connection with such a service; or any "constitutional corporation" that either manufactures, installs, maintains or supplies data processing devices for use, or likely to be used, in Australia, or develops, supplies or updates software that is capable of being installed on a computer or device that is likely to be connected to a telecommunications network in Australia. Some international internet-based companies and many Australian IT and internet businesses are likely to be classified as "designated communications providers" under one or other of the 15 categories in s 317C.

The notices and requests under the AA Act[7] aim to ensure the provider can supply the means to intercept and access the encrypted communications of the user base of that provider.

Technical Assistance Requests

Technical assistance *requests* are designed to have the provider cooperate with the security agency that issued the request on a 'voluntary' basis.[8] The 'voluntary' nature of assistance requests is linked to their exclusion from the compliance, enforcement and civil penalty provisions applying to technical assistance and technical capability *notices*.[9]

Requests are directed towards gaining an understanding of the capabilities of the recipient, and ensuring that the provider is capable of giving, and does give, certain sorts of help to an Australian agency in relation to their respective objects[10]:

> (a) in the case of Australian Security Intelligence Organisation (ASIO) — safeguarding national security; or
>
> (b) Australian Secret Intelligence Service (ASIS) — the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being; or

[5] Most of the 15 categories of "designated communications provider" are described merely as "persons" and not otherwise specified as to form, although the last two categories only cover "constitutional corporations", not "persons". Note also the unusual s 317ZT TA which purports to apply an 'alternative constitutional basis' to all of this new Part 15 as if all references to such providers were confined to those which are "constitutional corporations", perhaps indicating some doubt as to the constitutionality of casting the net so broadly.
[6] *AA Act* s 317D. "Electronic service" excludes broadcasting and datacasting services, but covers services which allow access to (or deliver) material over a carriage service to end users (or those with receiving equipment).
[7] Ibid ss 317A, 317G, 317L, 317T.
[8] Ibid s 317A.
[9] Ibid ss 317A Div 5, 317ZA and 317ZB.
[10] Ibid s 317A Table 1 Paragraph 2.

(c) Australian Signals Directorate (ASD) — providing material, advice and other assistance on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; or

(d) in the case of an interception agency[11] — enforcing the criminal law, so far as it relates to serious Australian offences; or

(e) in the case of an interception agency — assisting the enforcement of the criminal laws of a foreign country, so far as those laws relate to serious foreign offences.

Designated communication providers are incentivised to comply with a request by provisions protecting them from their customers seeking redress for any damage caused by compliance. The legislation provides immunity from civil liability in relation to cooperating with the request.[12] This immunity extends to the officers, employees or agents of the communications provider.[13] For example, this may apply to a large software company specialising in a mobile phone application if, as a result of complying with a request, it interferes with the mobile phone operating system or software environment, unintentionally rendering a customer's phone useless or defective.

This substantially reduces the legal avenues which aggrieved users of the communication provider can turn to for damage and harm caused to them as a result of the technical assistance request. Such damage could be commercial losses from lost business opportunities resulting from disrupted services, perceived exposure to increased risk of IT security breach, potential trade secret or commercial confidentiality violation, or apprehensions about privacy violations that are later proven unfounded. The immunity means that customers bear such losses alone, despite having no capacity to protect themselves from well-intentioned provider compliance efforts with unintended consequences.
Another factor distinguishing a technical assistance *request* from a technical assistance or capability *notice* is the principle in s 317ZK(3) that compliance with the latter is accompanied by a scheme for the state reimbursing extra provider costs above normal operating expenses (and preventing extra profits).[14] This means that unlike with *notices*, where the party seeking compliance covers the cost (subject to extensive exceptions), activities undertaken in compliance with a *request* are paid for by the provider, or in effect their customers. In this respect such 'voluntary' request-compliance activities expose the provider's customers to greater potential detriment than those undertaken in compliance with a notice, further extending the potential conflict of interest between provider and

[11] "Interception agency" means the Australian Federal Police, the Australian Crime Commission, or the Police Force of a State or the Northern Territory: s 317B TA. It thus includes certain state law enforcement agencies working in conjunction with or independently of federal agencies.
[12] Ibid ss 317G(1)(b), (c). See also s 317ZJ(1) for the similar, albeit slightly differently worded, civil immunity also attached to compliance with technical assistance notices and technical capability notices.
[13] Ibid s 317G(1)(d).
[14] This is similar to the exclusion of entities 'doing their best' to prevent offences under s 313 (1) and (2) from the reimbursement in s 314 that accompanies the mandatory compliance obligations in ss 313(3) and (4).

their customer, who bears both the risk of non-compensatable harm due to the immunity, and also an unspecified secret contribution to the provider's cost of compliance.

Companies are unable to defend themselves or inform their customers as the knowledge of receiving a notice or request is protected by non-disclosure penalty provisions that include a maximum 5 years imprisonment.[15]

It seems artificial to frame actions by the government designed to breach communications and data security as *requests* where non-compliance may result in the issue of a compulsory notice intended to achieve a similar aim.

Technical assistance requests may circumvent exceptions to assistance and capabilities notices. Technical assistance notices cannot be used to direct a designated communications provider into giving help to ASIO or an interception agency if it is not in connection with the activities of that provider.[16] Therefore, a technical assistance notice may not be able to order the development of new capabilities, but the issuing agency may be able to *request* the development of new capabilities. The same manoeuvring exists for technical capability notices, which cannot be used to compel a communications provider from removing electronic protections among other things.[17] These acts which would be unlawful if included in a *notice* may be subject to a *request*. The circumvention of these protective exceptions is a significant risk as they may leave communications providers vulnerable to third party intrusions.

Technical Assistance Notices

Technical assistance notices allow the Director-General of Security or the Chief Officer of an interception agency, without requiring the authorisation of a court, to issue a notice to a designated communications provider that requires them to perform acts that "are in connection with any or all of the eligible activities of the provider",[18] and are covered by the provision about giving help to the security agency, which includes:[19]

> (c) the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to:
>
> (i) enforcing the criminal law, so far as it relates to serious Australian offences; or

15 Ibid ss 317ZF(1)(c)(i), (ii), (iii) and (vi).
16 Ibid ss 317L(2A), (3).
17 Ibid ss 317T(4)(c)(i), 317E(1)(a).
18 Ibid s 317L(1)(a).
19 Ibid s 317L(2).

(ii) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or

(iii) safeguarding national security; or

(d) a matter that facilitates, or is ancillary or incidental to, a matter covered by paragraph (c).

Prior to a technical assistance notice being issued, the relevant agency must consult the provider,[20] unless the notice is determined to be issued in a matter of urgency[21] or the provider waives their right to consultation.[22] The security agency's assistance notice can be varied after it is given.[23] This suggests that once the security agency has consulted with the designated communications provider, it can change the notice to be more "effective". Technical assistance notices share a similar legislative scheme as technical assistance requests but *compel* the designated communication provider to assist.

Technical Capability Notices

The Attorney-General, with a request made by the Director-General of Security or the Chief Officer of an interception agency, and without judicial oversight, can issue a notice that requires a designated communications provider to do **any specified acts or things** that are in connection with the eligible activities of that provider.[24] A capability notice can compel the development of new capabilities to intercept information. In addition, the 'acts or things' requested in the notice must be directed towards ensuring the recipient of the notice is *capable* of giving certain forms of help to Australian security agencies to:[25]

(a) be directed towards ensuring that the designated communications provider is capable of giving listed help to ASIO, or an interception agency, in relation to:

(i) the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to a relevant objective; or

(ii) a matter that facilitates, or is ancillary or incidental to, a matter covered by subparagraph (i); or

(b) be by way of giving help to ASIO, or an interception agency, in relation to:

(i) the performance of a function, or the exercise of a power, conferred by or under a law of the Commonwealth, a State or a Territory, so far as the function or power relates to a relevant objective; or

(ii) a matter that facilitates, or is ancillary or incidental to, a matter covered by subparagraph (i).

[20] Ibid s 317PA(1).
[21] Ibid ss 317PA(2)(a), (3)(a).
[22] Ibid ss 317PA (2(b), (3)(b).
[23] Ibid s 317Q.
[24] Ibid ss 317T, 317T(1), 317C.

The relevant objectives of a technical capability notice are excessively broad as they relate to the enforcement of criminal law for 'serious' domestic offences,[26] and the enforcement of criminal laws for serious offences in foreign countries.[27] A serious criminal offence is any offence that can result in a punishment of 3 years imprisonment or more, or effectively any indictable offence under Australian state or federal criminal law.[28] A technical capability notice can have the broad objective of safeguarding national security, but it is not clear what this means or what limits apply.[29] Technical capability notices allow security agencies to review and potentially direct the development of new capabilities of a designated communications provider for the broad purposes of "intelligence gathering" justified by non-specific intentions.

Computer Access Warrants

The AA Act also includes an overhaul of computer access warrant powers.[30] The amendments widen the parameters of computer access warrants to include extraterritorial application, and increase protections for law enforcement.[31]

The AA Act amends computer access warrants through changes to the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Surveillance Devices Act 2004* (Cth), both of which provide for the application and administration of various forms of computer access warrants. What is most concerning is the expansion of the powers of the Attorney-General, without the need of judicial approval, to issue computer access warrants.[32] In addition, requests by foreign countries are funnelled through the Attorney-General.[33] Computer network operations such as these are subject to the limited oversight of executives.[34] Therefore the expansion of executive decision making powers represent a shift in which security agencies have almost exclusive authority over surveillance capabilities and the responsibility to oversee their use, without the benefit of independent judicial scrutiny.

ASIO Computer Access Warrants

The Attorney-General can issue a computer access warrant if satisfied that accessing data held in a target computer will substantially assist the collection of intelligence with respect to a security

---

[25] Ibid s 317T(2).
[26] Ibid s 317T(3)(a).
[27] Ibid s 317T(3)(b).
[28] Ibid s 317B.
[29] Ibid s 317T(3)(c).
[30] Ibid Sch 2, Part 1; *Australian Security Intelligence Organisation Act 1979* (Cth) ('ASIO Act'); *Mutual Assistance in Criminal Matters Act 1987* (Cth); *Surveillance Devices Act 2004* (Cth); *Telecommunications Act 1997* (Cth); and *Telecommunications (Interception and Access) Act 1979* (Cth).
[31] *AA Act* (n 2) s 47A.
[32] *ASIO Act* (n 30) s 25A.
[33] *AA Act* (n 2) s 15CC.
[34] Adam Molnar, Christopher Parsons and Erik Zouave 'Computer network operations and 'rule-with-law' in Australia' (2017) 6(1) *Internet Policy Review* 7.

matter.[35] For the purpose of these computer access warrants, relevant security matters include the protection of the people, the Commonwealth and the States and Territories from:[36]

i. espionage;
ii. sabotage;
iii. politically motivated violence;
iv. promotion of communal violence;
v. attacks on Australia's defence system;
vi. acts of foreign interference

Security also includes carrying out Australia's responsibilities to foreign countries in relation to these matters.[37]

The computers that can be subjected to a warrant are noticeably broad as this includes specific devices, computers on a particular premises or a computer associated with, used by or likely to be used by, a person whose identity may not even be known.[38] This far-reaching wording also extends to systems and networks.[39] In its broadest interpretation, systems and networks could include the internet in its entirety as the internet is a "network of computer networks".[40]

The AA Act expands the lawful methods of carrying out the objectives of a computer access warrant. It is permissible when deemed to be effective, to use any other computer or communication in transit to access the relevant data.[41] In addition, computer data or transitory communications can be added, copied, deleted or otherwise altered if considered necessary.[42] Communications that pass over telecommunications systems can also be intercepted.[43]

The most pronounced development in the legislative scheme is the increased levels of *remoteness* when accessing data. This is because computer networks and communications systems become larger sources of information and functionality than a single personal device specified in a warrant. There is an increased risk of these becoming 'general warrants', to which the US 4th Amendment is opposed, but to which Australian law offers little impediment.

---

[35] *ASIO Act* (n 30) s 25A(2).
[36] Ibid s 4 "Security".
[37] Ibid.
[38] Ibid s 25A(3).
[39] Ibid s 4 "Computer".
[40] Keiran Hardy 'Sweeping security law would have computer users surrender privacy' *The Conversation* (16 September 2014). https://theconversation.com/sweeping-security-law-would-have-computer-users-surrender-privacy-30041
[41] *ASIO Act* (n 30) s 25A(4)(ab)(i); *AA Act* (n 2) sch 2, Part 1, Amendment 4.
[42] *ASIO Act* (n 30) s 25A(4)(ab)(ii).
[43] Ibid s 25A(4)(b)(ba); *AA Act* (n 2) sch 2, Part 1, Amendment 6.

The expansion of computer access warrants is supported by new protections for law enforcement in the form of concealment of access provisions.[44] Pursuant to these laws, ASIO is authorised to do anything to conceal the fact that something has been done under a warrant.[45] The methods for concealment are analogous to the interception powers allowed under the Act. The specified computer can be removed and returned,[46] other communications from telecommunications systems can be intercepted,[47] other computers or communications in transit can be used, and data can be added, copied, deleted or altered.[48]

This legislative scheme grants ASIO the powers to intercept encrypted information when in transit. The legal standards controlling the issue of a warrant are complex but are non-specific, potentially allowing wider interception than what may be necessary. The incorporation of concealment provisions grants further interception and access powers to prevent the discovery of the initial interference.

Foreign Requested Computer Access Warrants

Computer access warrants under ASIO are domestic processes with international application. A similar legal framework exists for warrants sought by foreign governments that seek assistance through Australian surveillance laws in criminal investigations. Amendments to the *Mutual Assistance in Criminal Matters Act 1987* (Cth), also incorporated into the AA Act, allow for the Attorney-General to authorise a law enforcement officer to apply for a computer access warrant pursuant to the *Surveillance Devices Act 2004* (Cth) if the following conditions are met:[49]

> (a) an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of a foreign country (the ***requesting country***) that is punishable by a maximum penalty of imprisonment for 3 years or more, imprisonment for life or the death penalty has commenced in the requesting country; and
>
> (b) the requesting country requests the Attorney-General to arrange for access to data held in a computer (the ***target computer***); and
>
> (c) the requesting country has given appropriate undertakings in relation to:
>
> (i) ensuring that data obtained as a result of access under the warrant will only be used for the purpose for which it is communicated to the requesting country; and

[44] Ibid sch 2, Part 1, Amendment 7.
[45] *ASIO Act* (n 30) s 25A(8)(c).
[46] Ibid s 25A(8)(f).
[47] Ibid s 25A(8)(h).
[48] Ibid s 25A(8)(g).
[49] *AA Act* (n 2) s 15CC(1).

(ii) the destruction of a document or other thing containing data obtained as a result of access under the warrant; and

(iii) any other matter the Attorney-General considers appropriate.

The target computer can be a specified computer, a computer on premises or a computer associated with, used by or likely to be used by, a person whose identity may or may not be known.[50] The amendments are a legislative conduit to extraterritorial influence, and the international use of Australia's widening surveillance laws in other countries. This infrastructure can allow foreign governments to circumvent their own country's legal barriers by requesting Australian assistance. If approved, they benefit from less stringent laws.

Mutual Assistance and Computer Access Warrants

Computer access warrants for the purpose of a mutual assistance investigation can be subject to an application made by a law enforcement officer if they are authorised to do so under a mutual assistance authorisation.[51] The law enforcement officer must suspect on reasonable grounds that access to data held in a computer that relates to the commission of an offence, or the identity or location of the suspected person, is necessary to an investigation or investigative proceeding.[52] A deciding factor for an application is the perceived cogency of any potential evidence and intelligence, to the extent that it is possible to determine from information obtained from a foreign government that the warrant and authorisation applies.[53]

Computer access warrants obtained through the *Surveillance Devices Act 2004* (Cth) contain the same powers as a warrant obtained under the *Australian Security Intelligence Organisation Act 1979* (Cth).[54] There is little distinction between the surveillance conducted by Australian law enforcement agencies when acting on behalf of Australia and when assisting a foreign government**.** Additionally, the effects of a warrant granted under the Act are protected by concealment of access provisions.[55] The primary concern of this legislative arrangement is that it can be used in Australia to enforce foreign laws or conduct surveillance of domestic and foreign populations for foreign national interests.

[50] Ibid s 15CC(2).
[51] Ibid ss 27A(4), (4)(a).
[52] Ibid s 27A(4)(b).
[53] Ibid ss 27C(2), (2)(f).
[54] Ibid ss 27E(1), (2), (3).
[55] Ibid s 27E(7).

Issues and Concerns

The AA Act raises numerous concerns for the international community that need to be addressed. These include:

- **Vague and unclear limits on extraordinary powers**
  - The AA Act defines many of its powers with vague language. These include:
    - S317C "Designated Communications Providers". This definition is without limitation and could potentially include any person or company who provides services and materials using the Internet or telecommunications system with some Australian aspect.[56] This allows relevant agencies to issue technical assistance requests and notices to almost any organisation that utilises the internet.
    - The definition of "computer" for the purposes of Computer Access Warrants pursuant under the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Surveillance Devices Act 2004* (Cth) also has no constraint.[57] It includes computers, networks, systems or any combination of those, it is so broad that the entirety of the Internet could potentially fit within the definition.[58]

  These factors are unlikely to be subject to judicial review because of the absence of their consideration when warrants are granted. So, it leaves the rigorous scrutiny of this broad terminology to specific legal challenges that will only arise after criminal prosecutions are instigated, if at all.

- **Enforcement of laws of foreign countries / extraterritorial application**
  - **Information requests funnelled through Australia as 'weak link' in 'Five Eyes' alliance with only Western democracy with no enforceable human rights**
    - The AA Act expansion of the Attorney-General's powers in regard to the authorisation of foreign information requests bypasses the procedures and judicial inclusion set out by Mutual Legal Assistance Treaties (MLAT).[59] While the treaty system has been criticised for being inefficient,[60]

[56] Molnar, Adam et al. *Submission to the Department of Home Affairs on the Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, (September 2018) 10.
[57] *ASIO Act* (n 30) s 22; *Surveillance Devices Act 2004* (Cth) s 6 "Computer".
[58] Ibid.
[59] *AA Act* (n 2) s15CC.
[60] Lizzie O'Shea and Elise Thomas, 'The Role of Encryption in Australia, A Memorandum', *Access Now* (January 2018) 8. https://www.accessnow.org/cms/assets/uploads/2018/01/Crypto-Australia-Memo.pdf

circumventing the process altogether and ignoring legal jurisdictional barriers in favour of covert information sharing presents a myriad of issues:

- The potential to undermine the admissibility of evidence in criminal trials as MLAT protocols were established to mirror domestic criminal standards for international joint investigations.[61]
- Reducing the standard of due process.[62]
- The Act broadens what is permissible transnational surveillance and does so by making it an exclusively discretionary decision for the executive.

- Australia's unilateral collection of evidence pertinent to international interests may destabilise its diplomatic relations. While the Attorney-General can request that some undertakings be made (i.e. that the evidence issued solely for the purposes of the investigation for which it is being sought or the destruction of a document or thing *containing* data obtained as a result of access under the warrant), there is no way for Australia to enforce these undertakings once the data has been provided to foreign law enforcement agencies.[63]

– **In cases involving the death penalty, or offences not recognised in Australia**

- Australian cooperation in criminal investigations that may include the death penalty in a requesting foreign country is particularly concerning due to Australia's stance towards capital punishment.[64] Since the death penalty's abolition federally in Australia,[65] the government position has been the condemnation of state administered capital punishment.[66] Therefore, legislation creating the possibility of Australian complicity in matters involving the death penalty is in contradiction with Australian values and the explicit policy of previous Australian governments.
- The absence of limitations which restrict application of these new powers to only those matters which would be crimes in Australia ('dual criminality')

[61] Molnar, Adam et al. *Submission to the Department of Home Affairs on the Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, (September 2018) 27.
[62] Ibid.
[63] Ibid 27–28; *AA Act* (n 2) s15CC(c).
[64] *AA Act* (n 2) s 15CC(1)(a).
[65] *Death Penalty Abolition Act 1973* (Cth).

may similarly mean that these intrusive and dangerous powers may be open to use in pursuit of matters which are not accepted as 'criminal' by the Australian community or its legislators. Other countries still criminalise activities which are no longer offences, or serious offences, in Australia (for example, persecution and prosecution of various sexual or gender matters); and new offences are also being created elsewhere which cover activities not subject to criminal sanction in Australia (including political, religious, racial or ethnic matters).

- **Limited transparency and accountability**
  - **Reporting Requirements**
    - Technical Assistance Requests and Notices are not subject to substantial reporting, only requiring the number of requests and notices given to be included in an annual report.[67]
    - The reporting of Computer Access Warrants is the responsibility of the Director-General's of the relevant security agencies and handled internally.[68] Thus, this information is withheld from the public. This potentially conceals the use and incremental extension of actions, notices, requests and warrants authorised under these provisions to cover a much larger range of communications and data than may have been contemplated when the amendment was rushed through the legislature.
- **Expansion of executive powers internationally**
  - **No judicial oversight**
    - The AA Act's approach to handling foreign requests phase out judicial approval that was common practice when operating in accordance with MLAT procedures.[69] While this procedure is under-analysed in Australian research, judicial oversight is superseded by executive powers.
    - The implementation of Technical Assistance Requests and Notices are immune from judicial oversight as they have been excluded from the scope

---

[66] Department of Foreign Affairs and Trade, "Australia's Strategy for Abolition of the Death Penalty" (June 2018). <https://dfat.gov.au/international-relations/themes/human-rights/Documents/australias-strategy-for-abolition-of-the-death-penalty.pdf>.
[67] *AA Act* (n 2) s 317ZS.
[68] Molnar, Adam et al. *Submission to the Department of Home Affairs on the Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, (September 2018) 20-21.
[69] Mutual Legal Assistance Treaties, 'FAQ' *Access Now*. https://www.mlat.info/faq

of the *Administrative Decisions (Judicial Review) Act 1977* (Cth).[70] This removes contest by 'Designated Communications Providers' who oppose requests or notices on the grounds that they do not accept the decision maker's rationale – if that rationale is ever disclosed.

- The Attorney-General and executive decision makers are responsible for the approval of foreign requests for Computer Access Warrants and preventing the misuse of their powers. This is a clear conflict as they are tasked with self-policing in an environment with limited restrictions or public disclosure obligations.

- **Damage to Businesses, Workers and Consumers**
  - **Costs of Compliance**
    - The lack of legal recourse available to businesses that receive technical assistance requests and notices, and consumers who are aggrieved by compliance measures will reduce trust between businesses and consumers.
    - The financial costs that could burden small businesses or tech startups could damage their growth and development, thus having a negative impact on an economy or individual business. It does not appear that legislators considered previous examples of mass disruption of core internet services or disruption of particular functionality arising from incompetent or misguided application of existing Commonwealth agency powers under equivalent existing provisions like s 313 TA.
  - **Overseas Employment and Network Security**
    - Australian nationals who work overseas could be subject to an assistance order pursuant to s 64A, to assist law enforcement in accessing computers or computer systems that the national has worked on.[71] This could undermine trust and business relationships with Australia as well as risk Australian employment in online services internationally.

It should be noted that this is not an exhaustive list of concerns, and for further details please see the Australian Privacy Foundation joint civil society submission to the Exposure Draft of the AA Act, and subsequent submission to the Parliamentary Joint Committee on Intelligence and Security.

[70] *AA Act* (n 2) Sch 1, Part 1, Amendment 1.

Conclusion

We offer this report to help inform and educate international audiences about the global implications of the recently enacted telecommunications 'Assistance and Access' laws in Australia which draft a potentially wide range of people and businesses, from Australia and other countries, to undermine both the effectiveness of encryption tools and previous legal restraints on intrusive surveillance technologies, and gags them from revealing the extent of these new laws in practice. We call upon the international civil society community to partner with the Australian Privacy Foundation and others in seeking the repeal of this law.

Contact:

Dr Monique Mann
Board of Directors
Chair of the Surveillance Committee
Australian Privacy Foundation

[71] Ibid s 64A(2)(d)(vi)

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies https://privacy.org.au/publications/by-date/
- Media https://privacy.org.au/home/updates/
- Current Board Members https://privacy.org.au/about/contacts/
- Patron and Advisory Panel https://privacy.org.au/about/contacts/advisorypanel/

The following pages provide outlines of some of the campaigns that the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Census (2006) https://privacy.org.au/campaigns/census2006/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) https://privacy.org.au/campaigns/privacy-media/
- The MyHR (2012-) https://privacy.org.au/campaigns/myhr/
- The Census (2016) https://privacy.org.au/campaigns/census2016/