Comments to

the Department of Home Affairs

3 Lonsdale Street

Braddon ACT 2612

Re: Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

10 September 2018

[redacted]

Thank you for the opportunity to provide feedback to the Department of Home Affairs on the exposure draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018.[1] The issues, challenges, and opportunities for law enforcement in the digital era are both numerous and complex, and any legislation in this area will have significant impacts around the world.

Specifically, we would like to focus our comments on the overbreadth of the Assistance and Access Bill and its global implications for digital security. We will discuss the lack of an adequate factual record to justify the expansive authority provided in the Assistance and Access Bill and the availability of alternate methods to provide intelligence and law enforcement officials with the data necessary for investigations. We will also briefly discuss schedule 2 of the Assistance and Access Bill on government hacking and the need for greater discussion and safeguards. We conclude with a list of recommendations and suggestions for moving forward and hope to continue to engage in an open dialogue on these critical issues.

About Access Now and previous work

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[2] By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.[3]

At Access Now digital security is one of our primary focus areas. We have done extensive work related to cybersecurity, integrity of communications systems, government hacking, and the importance of encryption, including providing information and trainings for policymakers and the public on the importance of digital security and the protection of digital systems.[4] We also operate a 24/7 Digital Security Helpline that works directly with individuals and organisations around the world to keep them safe online, including through the provision of rapid-response

[1] https://www.homeaffa rs.gov.au/about/consu tat ons/ass stance-and-access-b -2018.
[2] https://www.accessnow.org/.
[3] https://www.accessnow.org/about-us/.
[4] *See e.g.*, https://www.accessnow.org/ ssue/d g ta -secur ty/.

emergency assistance.[5] In addition, Access Now supports grassroots activists around the world. We coordinate a global coalition in excess of 400 named organisations, experts, and companies from more than 60 countries in support of strong encryption.[6] Additionally, we host the Secure Australia coalition website.[7]

As part of these efforts, Access Now has facilitated greater multistakeholder dialogue on the topic of encryption. The Crypto Summit was a day long discussion on the history and uses of cryptography.[8] Crypto Summit 2.0 followed, a series of workshops and discussions to address significant questions surrounding the use of cryptography and law enforcement access, examine concrete outcomes, and identify areas for future discussion.[9] Finally the Crypto Colloquium was an invitation-only closed door convening of experts, advocates, former government officials, and company representatives in 2017 to examine a sample legislative proposal and its impact on law, economics, and security.[10] The Crypto Colloquium Outcomes Report identified areas of consensus within several key themes, including law and policy and security, as well as unanswered questions.[11]

In May 2018, Access Now was invited to provide expert testimony before the Joint Committee on Law Enforcement's inquiry into the impact of new and emerging information and communications technologies. We explained, "every proposal for a mechanism to allow law enforcement to bypass encryption has been found to have security flaws that could, if deployed, cause grave damage to people, governments, and infrastructure. It could also have knock-on effects that we cannot anticipate today."[12] However, we also noted, "[e]xperts have identified strategies to help law enforcement without undermining encryption."[13]

In July 2018, Access Now led 76 experts, organisations, and companies in a letter to Members of Parliament, explaining "in order to fully realise the benefits of the digital space, Australia must fully and unequivocally commit to a strong foundation for digital security."[14] In response, the Honorable Angus Taylor, Minister for Law Enforcement and Cybersecurity, clarified, "[e]ncryption is a vital security measure for digital data, and the Government is committed to strong protections for personal and commercial information."[15]

---

[5] https://www.accessnow.org/he p/.
[6] securethe nternet.org.
[7] https://secureaustra a.org.au/.
[8] https://www.accessnow.org/crypto_summ t_part1/.
[9] https://www.accessnow.org/crypto-summ t-2-0/.
[10] https://www.accessnow.org/governments-want-encrypt on-backdoors-new-report-exam nes- ega -po cy- mp cat ons/.
[11] https://www.accessnow.org/cms/assets/up oads/2018/02/Encrypt on- n-the-Un ted-States-Crypto-Co oqu um-Outcomes-Report.pdf.
[12] https://www.accessnow.org/test mony-before-the-par ament-of-austra a-par amentary-jo nt-comm ttee-on- aw-enforcement/.
[13] *Id*.
[14] *See* https://www.accessnow.org/g oba -coa t on-ca s-on-austra as-government-to-reject-p ans-to-underm ne-encrypt on/.
[15] https://www.accessnow.org/cms/assets/up oads/2018/08/s gned-response-from-M n ster-Angus-Tay or.pdf.

In addition to our below comments, Access Now has also joined two other submissions in response to the Assistance and Access Bill. Our observations here are supplemental to those raised in these other submissions.

Relevant Summary of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

The exposure draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (hereafter, "Assistance and Access Bill" or "the Bill") was published in August 2018 along with a detailed explanatory document.[16] The Assistance and Access Bill is broken down into 5 schedules.[17] Our comments focus on schedule 1 (Industry Assistance) and schedule 2 (computer access warrants etc.).

Schedule 1 provides for the issuance of three new instruments: Technical Assistance Requests (TARs), Technical Assistance Notices (TANs), and Technical Capability Notices (TCNs).

Technical Assistance Requests (TARs) and Technical Assistance Notices (TANs)

TARs are requests to designated communications providers to voluntarily do "acts or things" for which the Bill provides a waiver of civil liability.[18] TANs compel an entity to conduct one or more specified "acts or things."[19] Both TARs and TANS have to be issued in direct relation to, or as facilitates or is ancillary or incidental to, "the performance of a function, or the exercise of a power conferred by or under a law...so far as the function or power relates to" certain objectives.[20] The named objectives are similar for both TARs and TANS, including "enforcing the criminal law and laws imposing pecuniary penalties," "assisting the enforcement of the criminal laws in force in a foreign country," and "protecting the public revenue."[21] TARs can also be issued in "the interests of Australia's" national security, foreign relations, or national economic well-being,[22] while TANs can be issued for "safeguarding national security."[23]

TARs and TANs are both limited to the eligible activities of designated communications providers,[24] with definitions for both what entities constitute designated communications providers and what eligible activities are for each category of provider.[25] "Acts or things" are also defined, though TANs may be issued for acts or things outside of the provided definition.[26]

---

[16] https://www.homeaffa rs.gov.au/about/consu tat ons/ass stance-and-access-b -2018.
[17] https://www.homeaffa rs.gov.au/consu tat ons/Documents/the-ass stance-access-b -2018.pdf.
[18] Ass stance and Access B (schedu e 1) at 317G(c)-(d).
[19] *Id*. at 317L(1).
[20] *Id*. at 317G(2)(b)(v)-(v), 317L(2)(c)-(d).
[21] *Id*. at 317G(5)(a)-(c), 317L(2)(c)( )-( ).
[22] *Id*. at 317G(5)(d).
[23] *Id*. at 317L(2)(c)(v).
[24] *Id*. at 317(1)(a), 317L(1).
[25] *Id*. at 317C.
[26] *Id*. at 317E. *See also* 317L(3) ("The acts or th ngs that may be spec f ed n a techn ca ass stance not ce g ven to a des gnated commun cat ons prov der nc ude (*but are not limited to*) sted acts or th ngs" (emphas s added)).

TARs may be issued by the Director-General of Security; the Director-General of the Australian Secret Intelligence Service; the Director-General of the Australian Signals Directorate; or the chief officer of an interception agency, consisting of 10 named police or law enforcement entities as well as any Police Force of a State or the Northern Territory.[27] TANs may be issued only by the Director-General of Security or the chief officer of an interception agency.[28] Notably, any of these forces may delegate their authority, including to staff members of respective agencies.[29] In order to issue a TAN, the relevant Minister or officer, or their delegate, must be "satisfied that...the requirements imposed by the notice are reasonable and proportionate; and compliance with the notice is practicable; and technically feasible."[30] There is no formal process for the designated communications provider to contribute to or appeal such a determination.

Technical Capability Notices (TCNs)

TCNs are also issued to designated communications providers in connection to eligible activities.[31] TCNs can compel the commission of any of the acts or things defined by the bill, with the exception of "removing one or more forms of electronic protection that were applied by, or on behalf of, the provider," though they can also compel any additional act or thing as a Minister determines by legislative instrument.[32]

Under a TCN the acts or things must be directed toward "ensuring that the designated communications provider is capable of giving listed help to [the Australian Security Intelligence Organisation], or an interception agency" or "by way of giving help to" the same, either directly in relation to, or on a matter that facilitates, or is ancillary or incidental to, the "performance of a function, or the exercise of a power, conferred by or under a law...so far as the function or power relates to a relevant objective."[33] The list of relevant objectives is identical to that for TANs.[34]

While the Director-General of Security or the chief officer of an interception agency may request a TCN, only the Attorney-General can issue one, if satisfied that requirements are reasonable and proportionate and that compliance is practicable and technically feasible.[35] The Bill requires at least 28 days notice, though it can be waived or avoided in certain situations.[36] During this time, Designated Communications Providers may "make a submission...on the proposed notice" that must be considered.[37] However, there is no formal appeal process beyond this consultation.

---

[27] *Id.* at 317G(1)(a), 317ZM.
[28] *Id.* at 317L(1).
[29] *Id.* at 317ZN-317ZR.
[30] *Id.* at 317P.
[31] *Id.* at 317T(1).
[32] *Id.* at 317T(4)(c), 317T(5).
[33] *Id.* at 317T(2).
[34] *Id.* at 317T(3).
[35] *Id.* at 317T(1), 317V.
[36] *Id.* at 317W.
[37] *Id.* at 317W(1)(a)( ), 317W(1)(b).

Computer Access Warrants

Schedule 2 provides for computer access warrants for the purpose of searching a particular computer, a computer on a particular premises, or a computer associated with, used by, or likely to be used by a known or unknown person, with "computer" meaning one or more computers, computer systems, or computer networks (or any combination of the three).[38] This includes computers in a foreign country if the person executing the warrant will be physically located in Australia and the location where the data is held is unknown *or* cannot be determined.[39]

Broadly speaking, an application for a computer access warrant is evaluated by a Judge or a nominated Administrative Appeals Tribunal ("AAT") member, though in most cases the evaluating entity is not asked to substantively evaluate the application to determine if it meets the necessary standards.[40] Instead, the Judge or AAT member is only asked to determine if there are reasonable grounds that gave rise to the application, though they are required to have regard for the privacy of any person likely to be affected, the existence of alternative means of obtaining evidence, and the value of the information sought, among other things.[41]

A computer access warrant may authorise any things considered appropriate by the judge or AAT member.[42] The warrant also authorises the commission of a broad range of identified acts in order to ensure that actions taken under it remain secret.[43]

I. The Assistance and Access Bill will have far-reaching impacts that undermine digital security and human rights for users around the world

Schedule 1 of the Assistance and Access Bill creates new authorities that can be exercised broadly without appropriate legal standards or necessary safeguards. If exercised as written these authorities will have a deleterious impact on digital security while actually increasing the potential for criminal activity.

Below we briefly evaluate how schedule 1 creates significant loopholes and ambiguities at nearly every stage of the process it establishes to issue TARs, TANs, and TCNs.

Listed Acts or Things

The scope of the "acts or things" that could be requested (under TARs) or compelled (under TANs or TCNs) is significant, implicating software code and hardware specifications, physical access to equipment or property, deployment of malicious code, shifting entire internal systems,

[38] Ass stance and Access B (schedu e 2) at 37, 15CC(2), 36.
[39] *Id*. at 43A(4).
[40] *Id*. at 27C.
[41] *Id*.
[42] *Id*. at 27E(2).
[43] *Id*. at 27E(7)(c).

or undermining encryption technologies or algorithms (more on this below). Additionally, despite that the definition of "acts or things" specifically exempts the making of a false or misleading statement or misleading conduct, it may also include fraudulent activity, including material omissions of fact as well as to the extent activity must be undertaken to ensure the secrecy of any TAR, TAN, or TCNs issued. Additionally, as discussed above, both TANs and TCNs can be issued to compel activity outside of the already broad scope of the definition of acts or things.

Not only will the far reach of this section cause the judgment of experienced security engineers to be substituted for that of government officials without any requirement for consultation or independent technological review, but it also conscripts engineers into civil service by compelling assistance with government research, development, and testing. This undermines the levels of security companies may provide to users and consequently interferes with human rights. In addition, it could cripple the vibrant internet ecosystem that Australians enjoy today.

Designated Communications Providers

The scope of "qualifying communications providers" predictably includes major technology companies like Google, Twitter, and Facebook and large telecommunications companies like Telstra, Vodafone, and Verizon. However it also includes any website operator with an end-user located in Australia, including news and journalism websites and digital storefronts, presumably even if the person is not a resident or domicile of Australia.[44] It also includes any service utilised by any of these companies, potentially encompassing any B2B provider, including cybersecurity and data analytics companies.[45] The financial and administrative burdens the exercise of these provisions could place on these entities would be felt more acutely. It could also prevent new entrants into certain sectors, dimming competition that benefits end users.

Issuance of TARs and TANs

As discussed above, while only certain Ministers and officials are granted the authority to issue TARs and TANs, they are also able to delegate that authority to a broad range of other officials and staff. At Access Now's Crypto Colloquium in 2017, participants reached consensus that a mechanism that would be used frequently or one that could be used by more people would have a higher risk of being exploited.[46] Leaving open the potential for expansive delegation could increase the complexity, and consequently the insecurity, of any given access mechanism.

Purpose and Objectives

TARs, TANs, and TCNs can be invoked not only as directly related to the performance of a legal function or power, but also to facilitate such function or power or as "ancillary or incidental" thereto. This purpose specification allows the authorities to be exercised with only the vaguest

[44] *See* Ass stance and Access B (schedu e 1) at 317C(4)-(5).
[45] *See e.g. Id.* at 317C(6)-(7).
[46] https://www.accessnow.org/cms/assets/up oads/2018/02/Encrypt on- n-the-Un ted-States-Crypto-Co oqu um-Outcomes-Report.pdf.

connection to the pursuit of a legal objective, drawing tenuous connections between the means sought and the ends to be achieved. Compounding this vagueness, the identified objectives themselves are exceptionally broad without necessary limitations or explanation.

For example, the objective of "enforcing the criminal law," could be used for any crimes, including consorting, public drunkenness, and posting bills or defacing property. Additionally, the explanatory document makes clear that this authority could be exercised to "support the investigation...of suspected offences," potentially green-lighting massively invasive fishing expeditions into computer networks and systems.[47] The objective of "safeguarding national security" also carries potential for abuse. Governments around the world invoke "national security" to justify massive interferences with the exercise of human rights.[48] The Council of Europe has questioned this practice, asserting "it is becoming increasingly clear that secret, massive and indiscriminate surveillance programmes are not in conformity with European human rights law and cannot be justified by the fight against terrorism or other important threats to national security. Such interferences can only be accepted if they are strictly necessary and proportionate to a legitimate aim."[49] By including this catch-all with no further limitation, Australia is contravening basic human rights principles while creating a foreseeable conflict of laws with other jurisdictions.

Legal Standards and Review

In order to issue a TAN or a TCN, the issuer has to be satisfied that it is reasonable and proportionate and compliance is practicable and technically feasible, though this is not subject to any further review or appeal. This standard and process is inconsistent with international human rights law on its face.[50] Not only does it fail to require that the Notice is necessary to respond to a legitimate government aim, but by not requiring approval by a competent judicial authority the Bill drastically increases the potential for misuse and abuse.

The basic lack of adequate transparency, not to mention comprehensive secrecy provisions that prevent disclosure of the existence of the Notice and criminalise any attempt to disclose material related to it, compounds the failures of the Bill by preventing both individual notice to those impacted as well as public accountability for the ways in which the provisions are used.

Enforcement

Within the scope of enforcement, the Assistance and Access Bill provides that a person must not: "aid, abet, counsel, or procure a contravention of [a TAN or TCN]; induce...a contravention

---

[47] https://www.homeaffa rs.gov.au/consu tat ons/Documents/exp anatory-document.pdf at 31.

[48] *See e.g.* http://news.bbc.co.uk/2/h /sc /tech/1357513.stm; https://motherboard.v ce.com/en_us/art c e/534pmd/how-an- ega -canad an-spy-program-sa ed-through-regu atory-checks-opc-odac-cs s; https://www.nyt mes.com/roomfordebate/2013/06/09/ s-the-nsa-surve ance-threat-rea -or- mag ned ("Nat ona secur ty (and other government nterests) may just fy some narrow ntrus ons on pr vacy n some c rcumstances. The prob em w th the programs d sc osed over ast week s that they are so aston sh ng y broad.").

[49] https://rm.coe. nt/16806da51c at 16-17.

[50] *See e.g.*, https://necessaryandproport onate.org/pr nc p es.

of [a TAN or TCN]; be in any way, directly or indirectly, knowingly concerned in, or party to a contravention of [a TAN or TCN]; or conspire with others to effect a contravention of [a TAN or TCN]."[51] Taken together, this provision could be used to punish advocacy efforts that oppose the Bill or its provisions or speech critical of its use. It could also have harsh implications for "open source" tools and services that would allow users to directly observe any changes in code.

Specific Impacts on Encryption and Digital Security

In addition to the aforementioned provisions that extend the reach of the Assistance and Access Bill far beyond what could be considered to be legitimate uses, it is foreseeable that the Bill will be used in a way that will impact global digital security.

This submission has explained how the definition of listed acts or things is overbroad generally. In addition, a TAN could be used to compel a Designated Communications Provider to remove "one or more forms of electronic protection," which, depending on the nature of the service, could undermine encryption more broadly since many systems could not strip protections for only a single user or may require broader changes in order to facilitate access.

While TCNs are not permitted to be used in this way, there are other ways that TCNs may be used to undermine security. For example, encryption keys could be required to be disclosed or stored in certain places, increasing the chances for exploitation. Additionally, services could be pushed to use a weaker form of encryption or develop on top of compromised or weak security protocols to facilitate access. All of these activities would seriously damage the security and efficacy of encrypted systems. Finally, companies and services may even choose not to develop or implement security tools or technologies that Australian security or police agencies would seek to interfere with, chilling security research and development globally.

Taken together, the activities TANs and TCNS could compel would increase the potential for exploitation and introduce new threat vectors. While some of these primary and secondary impacts may be foreseeable, there is no requirement in the Assistance and Access Bill for a technical review by an expert who knows how to communicate with private sector engineers before a TAN or TCN is issued. However, other effects may be so unpredictable that such technical review would be ineffective. These impacts could be aggravated when the authorities in schedule 2 are introduced. These authorities empower Australian government agencies to develop and grow their hacking capacities without vital and necessary protections. In order to respect human rights, government hacking must come with strong safeguards given the high risk of harm. These are not included in the Assistance and Access Bill.

Finally, while it is laudable that the bill does specifically prohibit the government from mandating a systemic weakness in an encrypted system, the term "systemic" grants the government leeway to undermine specific encrypted systems. The ambiguity in the threshold of "systemic"

[51] *See* Ass stance and Access B (schedu e 1) at 317ZA(2).

interference could still allow authorities to compel a range of activities under the Bill that could have broad impact and thereby undermine user trust in companies and systems. That distrust could result in more unpatched systems and overall harm to cybersecurity, which would undoubtedly lead to an increase in data breaches and theft of digital devices, including smartphones and laptops.

II. There is an insufficient factual record to justify the implementation of the Assistance and Access Bill, particularly in light of its potential ramifications

As explained at length, the authorities to issue TARs, TANs, and TCNs are far-reaching and could have global impact. Such authority should be supported by a comprehensive factual record explaining what problem the authority is seeking to solve and the connection between the solution and the problem. However, the explanatory document published alongside the Assistance and Access Bill only provides vague references to how encryption is used without the necessary details to justify the incursions the Bill would authorise.[52]

For example, the explanatory document explains that "95 per cent of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications." However, it doesn't say what type of encrypted messaging that is or what type of information it prevents access to. Additionally, the document does not provide any information about the presumptive targets who are using encryption. Presumably, technically sophisticated potential terrorists would likely respond to the Assistance and Access Bill, or anything like it, by switching to services outside of Australia's jurisdiction. On the flip side, an authority as comprehensive as the Assistance and Access Bill is probably not necessary to effectively pursue those who are less sophisticated.

One area of consensus at Access Now's Crypto Colloquium was that it is hard "to proffer any solution without a set problem" and that "there is not enough information publicly available regarding the rate or frequently of cases in which encountering encryption has impeded an investigation." More information should be required before such drastic steps are pursued.

III. Alternative options are available to assist law enforcement in obtaining information necessary for investigations

Perhaps the biggest failure of this legislation is that it does not address issues that could markedly improve law enforcement's abilities in the digital era. There are many questions at the intersection of crime and technology. As the Joint Committee on Law Enforcement has seen in their examination of law enforcement in the digital era, these problems can include difficulties accessing data, lack of awareness regarding what data exists, difficulty accessing data oversees, and slow processes for interacting with technology companies that hold the data.

[52] https://www.homeaffa rs.gov.au/consu tat ons/Documents/exp anatory-document.pdf.

More information could help identify and fill these policy gaps and inform the public debate regarding lawful access to data. For example, corporate representatives could teach officers the most expedient ways to lawfully request information they already have authority to receive, including metadata as well as communications content when pursuant to the proper legal process. This is a process many companies have already initiated.[53] Other options to pursue include education for law enforcement about 1) what data actually exists and where to access it; 2) how to properly submit data requests to companies at scale; 3) paths to obtain data from companies overseas, and particularly the delays involved in the Mutual Legal Assistance (MLA) process, and 4) how to use certain types of date in legal proceedings.

These are issues that the Department of Home Affairs could address without undermining encryption and cybersecurity. And in fact, the emphasis at Home Affairs on encryption has meant that there has been little progress on these other issues. Just recently, the United States passed new legislation that enables the U.S. Department of Justice to negotiate bilateral treaties to allow foreign government officials to apply their domestic laws directly to access data held by a company in the United States. Under current law, Australia is not taking advantage of its relationship with the United States. While the new law itself fails to provide adequate protections, and any arrangement under this legal authority should include additional human rights protections, an agreement would grant Australian law enforcement significantly greater access to digital data.

IV. Schedule 2 of the Assistance and Access Bill should be reserved for further discussion and debate in order to determine the full breadth of its potential impact

Government hacking is one of the most invasive government surveillance activities in the modern world. All government hacking substantially interferes with human rights, including the rights to privacy and freedom of expression. While in many ways this interference may be similar to more traditional government activity, the nature of hacking creates new threats to human rights that are greater in both scale and scope. Hacking can provide access to protected information, both stored or in transit, or even while it is being created or drafted. Exploits used in operations can act unpredictably, damaging hardware or software or infecting non-targets and compromising their information. Even when a particular hack is narrowly designed, it can have unexpected and unforeseen impact.

There is also a great potential for international government hacking to raise conflicts of laws and to be used as an end-run around the protections built into Mutual Legal Assistance Treaties (MLATs), which are the primary legal instruments for government officials to obtain data stored in other jurisdictions. The Assistance and Access Bill amplifies the potential for these abuses by explicitly allowing cross-border hacking operations in cases where the location of a computer is unknown, incentivising forced ignorance with the reward of invasive search authority.

[53] *See e.g.*, https://www.wash ngtont mes.com/news/2018/sep/5/app e-team-w -tra n- aw-enforcement-d g ta -fore/.

Based on analysis of human rights law, for the above mentioned reasons among others Access Now has concluded that there must be a presumptive prohibition on all government hacking. Unfortunately Schedule 2 not only continues to authorise government hacking in Australia but expands the authority beyond the scope where it exists today. There is little information available for how Australia uses its current government hacking authorities and there has been insufficient conversation about plans to expand that authority or the intent of schedule 2.

Before schedule 2 is implemented in law, the relevant Ministers should provide more information on previous hacking operations and how the new provisions will supplement and interact with the current law. Additionally, effort should be made, separate from the conversation around the material in schedule 1, to facilitate public debate and discussion over the need for and scope of the schedule 2 material.

Recommendations

In light of the forgoing, Access Now provides the following recommendations for any further consideration of the Assistance and Access Bill. Our general recommendations set forth a potential path forward to ensure greater consideration and respect for human rights. However, we also offer more specific recommendations in regard to schedule 1 in the alternative. These recommendations do not mean to imply that we think that schedule 1 as it is written can be necessarily amended in a way that would comply with international human rights law. However, in the recognition that there may not be another opportunity to comment, we want to at least provide some clarity on ways that we believe the Bill could be improved. We do not offer the same suggestions in regard to schedule 2 and strongly believe that more time should be given for public consultation of this invasive and potentially harmful proposed authority.[54]

General recommendations

- Schedule 1 and schedule 2 should be intentionally divorced from one another and considered separately and with intention to provide full and complete understanding of how each will operate in the current legislative environment;
- Given its hithertofore absence from public debate, consideration of schedule 2 should be postponed for further debate and additional opportunity for public comment pending the availability of information that would further contribute to the understanding referenced above;
- Intelligence and law enforcement officials should provide additional information, including statistics and research, about the specific circumstances where schedule 1 would be invoked, including in regard to where and when encryption is hindering investigations and the goals sought through legislation;
- Subject to the data released in response to the above recommendation, members of Parliament and other leaders should actively consider, in consultation with industry and

[54] However, f no further t me s g ven for cons derat on, members of Par ament shou d cons der the safeguards sted n Access Now s report on "a Human R ghts Response to Government Hack ng," ava ab e at https://www.accessnow.org/cms/assets/up oads/2016/09/GovernmentHack ngDoc.pdf.

members of civil society and of the public, alternatives to schedule 1 that would provide intelligence and law enforcement officials with the data and information necessary for authorised investigations, including increased funding for trainings and reform of Mutual Legal Assistance Treaties;
- In order to prepare for the continued development of technology and protect Australians against criminal activity in the digital age, Australia should commit to meaningfully investing in public research and development of new and more sophisticated digital security tools and services, including through grants to independent experts and technologists.

Specific Recommendations on Schedule 1

- The definition of "listed acts or things" should be limited to protect personal autonomy and avoid any fraudulent activity. Private individuals should not be forcibly conscripted to build tools or technologies for government agencies nor should individuals or companies be compelled to turn over information that could precipitate a malicious intrusion on their networks or systems. In order to ensure the integrity of systems and communications, 317E(1)(a) should be specifically stripped from the Bill. Finally, TANs and TCNs should be limited to the actions within the definition, subject to amendment by Parliament;
- Designated communications providers should be substantially limited to both those who have a tangible, direct connection to Australia as well as those who are in an economic position to comply with notices;
- The list of officials to whom authority to issue TARs or TANs can be delegated should be substantially limited and tracked, subject to regular publication and review;
- Purposes for which requests or notices may be issued should be specifically related to the pursuit of a legitimate government aim, which should be specified in detail to include only serious crimes or specified national security interests. Compliance with foreign law should be stripped from these provisions unless additional protections are added to ensure that the foreign law meets human rights standards;
- The issuance of a TAN or TCN should require, at a minimum, a demonstration of strict necessity and proportionality to a legitimate government aim and subject to review by a competent judicial authority operating independently of any intelligence or law enforcement agency or organisation. Those served with TANs and TCNs should have the legal right to appeal the issuance of a TAN or TCN to the same judicial authority and have the ability to notify impacted users. Additionally, the Bill should include greater rights to publish information on the receipt of TARs, TANs, and TCNs, as well as requirements for government agencies and departments to regularly publish significantly greater statistics on the use of the authorities, including cases in which they are used and the extent they contributed necessary information to investigations;
- Agencies or offices with authority to issue TARs, TANs, or TCNs should be provided with additional resources in the form of employees with technical expertise whose sole job is to consult on the acts or things requested or compelled from Designated Communications Providers;

- Section 317ZA(2) should be stripped entirely from the Bill. Additionally 317ZF, criminalising specifically the unauthorised disclosure of any TAR, TAN, or TCN information, should also be stripped or qualified with an allowance for whistleblowing activities conducted in the public interest to reveal waste, fraud, abuse, or unlawful activity;
- The limitation against TANs or TCNs with the effect of requiring the implementation or building of a systemic weakness or preventing a systemic weakness from being rectified should be clarified to ensure it includes any action that would have indiscriminate impact on users of a certain system, tool, or technology as well as any activity that would indiscriminately impact the implementation or use of encryption, including key escrow schemes, or build capabilities that could be used to bypass encryption protections.

Conclusion

Thank you for consideration on this important issue. We appreciate your time and attention. If you have any questions about this submission or any other issues raised by the Assistance and Access Bill you can contact [redacted] at [redacted] or [redacted] at [redacted].