October 2019

Dr James Renwick CSC SC
Independent National Security Legislation Monitor
12/174 Phillip St
Sydney, NSW 2000
Phone: (02) 9232 8545

By email: INSLM@inslm.gov.au

Dear Dr Renwick,

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

Thank you for your letter dated 22 August 2019 in which you requested Access Now to make a formal submission to your review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act*.

As you will be aware, Access Now has been actively engaged in consultation of TOLA since early 2018 before the full text was introduced. We appreciate the opportunity to express our concern over the powers enshrined in this legislation, especially given the focus of the review on the necessity and proportionality of the Act, as well as the rights of individuals. In order to support your review, we are attaching the following documents which we have previously presented to the Parliament in an annex to this letter:

- Access Now testimony to the Parliamentary Joint Committee on Law Enforcement, 11 May 2018
- Access Now submission to the PJCIS *Inquiry on Telecommunications and Other Legislation Amendment*, 22 February 2019
- Access Now submission to the PJCIS *Review of the Amendments Made by the Telecommunications and Other Legislation Amendment*, 12 July 2019

Additionally, we'd like to take this opportunity to draw your attention to the international coalition we convene hosted at securetheinternet.org, which presents an open letter signed by more than 300 organizations, companies, and experts internationally. This letter, which we submitted to the initial parliamentary inquiry, explains how encryption is central to the protection of human rights, the digital economy, and the preservation of cybersecurity.

We appreciate this opportunity for comment and look forward to supporting your office throughout the course of the Review.

Best regards,

Lucie Krahulcova
Policy Analyst, Australia and Asia Pacific
Access Now

ANNEX: Access Now contributions to the Parliament of Australia regarding TOLA (Assistance and Access Act)

Testimony before the Parliament of Australia: Parliamentary Joint Committee on Law Enforcement

11 MAY 2018 | 8:48 AM

The Australian government, like many around the world, is wrestling with issues about how to adapt law enforcement to the digital era. On May 11, 2018, two of Access Now staff testified before a parliamentary inquiry examining these issues, focusing on encryption. Their prepared testimony is below. Testimony and the following discussion is available for download here.

May 11, 2018
Thank you for the opportunity to address the Joint Committee on Law Enforcement's inquiry on the impact of new and emerging information and communications technologies. And thank you and the Secretariat for allowing us to speak with you remotely.
We are Nathan White and Amie Stepanovich of Access Now. Access Now is an international civil society organization established in 2009 to defend and extend digital rights of users at risk around the world.

At Access Now digital security is one of our primary focus areas. We operate a 24/7 Digital Security Helpline that works with individuals and organizations around the world to keep them safe online, including to improve digital security practices and provide rapid-response emergency assistance. We have done extensive work related to cybersecurity, integrity of communications systems, government hacking, and the importance of encryption, and that is what we would like to discuss here today.

We have developed significant experience on the topic of encryption. Among other things, Access Now has organized three events on the topic, including a private multi-stakeholder roundtable at the end of 2017 with technologists and members of the Obama Administration. We also convene the international coalition hosted at securetheinternet.org, an open letter signed by more than 300 organizations, companies, and experts internationally. This letter, which we submitted to the present inquiry, explains how encryption is central to protection for human rights, the digital economy, and the preservation of cybersecurity. Further, we published "The Role of Encryption in Australia," a report authored by Lizzie O'Shea and Elise Thomas and submitted to this inquiry. The report establishes the importance of encryption

specifically in the Australian context, also showing the necessity of encryption to preserving Australia's national security and the potential harm that could be caused by weakening encryption.

For our testimony today we want to reiterate four points from these submissions and our prior work:

1. Encryption is important – it provides the foundation for our digital world, and in a country like Australia, where nearly 90% of the population has access to the internet, encryption is essential for protecting not only the cybersecurity of connected critical infrastructure, but also protecting its people from criminal activity online.
2. Undermining encryption hurts security – 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.
3. Undermining encryption will not solve law enforcement's problems – principles of sovereignty and criminal incentives will likely drive law enforcement targets toward tools and technologies that are beyond the reach of any mandated access mechanism, leaving those who are less technically sophisticated or financially privileged to bear the brunt on any insecurity caused by a mandate; and finally
4. There are other means to assist law enforcement – there are many questions at the intersection of crime and technology, and as this committee has recognized, those questions cannot be addressed in a silo. These topics require careful consideration and investment, including in education and training for law enforcement and research into rights-respecting mechanisms to streamline cross-border requests for data needed. Experts have identified strategies to help law enforcement without undermining encryption. While these would have to be evaluated for their impact on human rights, they provide a better starting point for these conversations and a good path for further investigation.

Thank you again for the opportunity to appear before you today. We look forward to your questions.

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
VIA email: pjcis@aph.gov.au and portal: www.aph.gov.au/pjcis

21 February 2019

Re: Inquiry on Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ("Assistance and Access Act")

To Whom It May Concern,

Passed in December 2018, the Assistance and Access Act poses a grave risk to human rights and digital security around the world.[1] The Act should be fully repealed in order to ensure adequate time for a full consideration of the breadth and scope of its provisions, which did not happen prior to passage. However, absent a repeal, it is vital that it is quickly and substantially amended to limit these risks, and others, including risks to Australia's national security and digital economy. The potential for the Assistance and Access Act to be used in damaging, or even life-threatening, ways will only increase as more devices, appliances, and basic infrastructure, including bridges and electricity grids, become internet-operated and enabled.

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] In 2018, Access Now published a report on "Human Rights in the Digital Era" evaluating Australia's role in the international community.[4]

During its short pendency, Access Now produced three submissions regarding early drafts of the Assistance and Access Act.[5] In September 2018, we commented to the Department of Home Affairs on the consultation draft, highlight its overbreadth and implications for digital security.[6] When the Act was introduced, mere weeks later, and without any response to the thousands of comments submitted, we submitted comments to the Joint Committee

[1] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, No. 148 (2018), *available at* https://www.legislation.gov.au/Details/C2018A00148. Hereinafter, "Assistance and Access Act" or "the Act."
[2] *See* https://www.accessnow.org/.
[3] *See* https://www.accessnow.org/about-us/.
[4] *See* https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf.
[5] Experts at Access Now were also invited to testify prior to the publication of a draft of the bill. *See*, accessnow.org/testimony-before-the-parliament-of-australia-parliamentary-joint-committee-on-law-enforcement/.
[6] accessnow.org/cms/assets/uploads/2018/09/Access-Now-Assistance-and-Access-Bill-submission.pdf.

on Intelligence and Security, with specific recommendations to improve the proposal.[7] We also signed on to comments from a coalition of groups highlighting several deficiencies in the bill.[8] Access Now followed up with a final submission in November 2018, emphasizing the lack of factual record available in support of extraordinary powers contained in the bill, and imploring the Committee to delay its consideration until basic questions could be answered.[9]

Unfortunately, throughout these consultations those in support of the bill continued using fear tactics to press it forward.[10] The bill was ultimately pushed through passage in late December with only minimal changes. The passage of the Act garnered attention of the international community. However, there was a single bright spot in the Act's passage: a promise of further review of the Act in 2019, which poses a landmark moment for the Australian Parliament to remedy the text and demonstrate that it is possible to address modern challenges with rights respecting policies.[11] We hope that the Committee will take this opportunity, at a minimum, to remedy the most egregious parts of the grossly overbroad Act.

Require approval of all authorities by an independent judicial authority

International human rights law requires "determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent."[12] It is beyond questions that the Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) created by the Assistance and Access Act relate to communications surveillance, most directly by facilitating its commission. However, the provisions of the Assistance and Access Act that create these authorities do not require judicial approval, or even judicial involvement.[13] The consequence is that government officials with the authority to issue TANs and TCNs are given nearly unchecked power to unilaterally approve invasive activities with unpredictable and potentially dangerous

[7] *See* https://www.accessnow.org/cms/assets/uploads/2019/02/Sub33.pdf.
[8] *See* https://www.efa.org.au/main/wp-content/uploads/2018/10/Submission-Assistance-and-Access-Bill-2018_collaborative_submission.pdf, https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Comments_on_Australia_Assistance_and_Access_Bill_2018_10-11-18.pdf, https://www.commsalliance.com.au/Documents/releases/2016-media-releases3/2018-media-release-27, https://newamericadotorg.s3.amazonaws.com/documents/Coalition_comments_on_Australia_bill.pdf. *See also* https://www.efa.org.au/main/wp-content/uploads/2018/07/Australia-Encryption-Coalition-Letter.pdf.
[9] *See* https://www.accessnow.org/cms/assets/uploads/2019/02/Sub33.1-2.pdf.
[10] *See, e.g.*, https://www.theguardian.com/australia-news/2018/nov/26/asio-says-it-urgently-needs-powers-forcing-telcos-to-help-break-phone-encryption; https://www.zdnet.com/article/australian-government-accuses-labor-of-backing-terrorists-on-encryption-busting-bill/.
[11] *See* https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct.
[12] Necessary and Proportionate Principles, Competent Judicial Authority, *available at* https://necessaryandproportionate.org/principles#principle6.
[13] The use of the authorities would only involve a judge when used in connection with an existing authority with a requirement for judicial approval, though the approval would be limited to the utilisation of that authority. Conversely, all other uses would be unilaterally authorised and exercised.

outcomes.[14] Moreover, the Act fails to provide adequate right to a legal appeal. Taken together, this means there is very limited opportunity to challenge the lawfulness of a TAN or TCN.[15] Even worse is that the Act contains provisions for the delegation of authority to issue TANs and TCNs to an even greater number of officials, compounding the probability that the Act will be misused or used in ways that have severe unexpected or unintended consequences.

Recommendations:

- The Assistance and Access Act must be amended to require all TANs and TCNS to be approved and issued by a competent judicial authority who is impartial and independent. The judge should have the authority to examine the full scope of an application and to issue a ruling both regarding the extent it meets the requirements of the Act for containing the proper elements, including a specifically identified objective, as well as if it satisfies the standard for the notice to issue.
- Parliament must add new provisions to provide designated communications providers a right to appeal any TAN or TCN to a court of review on an allegation that the judge who issued the authority applied the standard improperly.
- Involvement of a judge should extend beyond issuance of notices to also include extensions, variances, renewals, as well as any request for the designated communications provider for a notice to be revoked on the basis of a material change in circumstances that impacts its development or use.
- Provisions allowing delegation of issuance of TANs and TCNs, as well as Technical Capability Requests (TARs), should be removed. In the alternative, delegation must be limited to only the most senior officials and only in limited, enumerated circumstances.[16] Special accountability mechanisms should be included to track delegations and publish information on the use of TARs, TANs, and TCNs by delegated officials.

Limit ability to invoke the authorities on behalf of foreign governments

The Assistance and Access Act allows that TARs, TANs, and TCNs may be invoked in pursuit of "assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offenses."[17] Serious foreign offenses are defined to

[14] Assistance and Access Act § 317L(1) ("The Director-General of Security or the chief officer of an interception agency may give a designated communications provider a notice, to be known as a technical assistance notice, that requires the provider to do one or more specified acts or things..."); Assistance and Access Act 317T(1) ("The Attorney-General may, in accordance with a request made by the Director-General of Security or the chief officer of an interception agency, give a designated communications provider a written notice, to be known as a technical capability notice, that requires the provider to do one or more specified acts or things").
[15] In regard to TCNs, the provider may request an assessment, but the scope of that assessment is limited, as is its ability to impact the final decision to compel the provider to act. *See* Assistance and Access Act § 317WA. ("If a consultation notice is given to a designated communications provider under subsection 317W(1) in relation to a proposed technical capability notice, the provider may, within the time limit specified in the consultation notice, give the Attorney-General a written notice requesting the carrying out of an assessment of whether the proposed technical capability notice should be given."; "the Attorney-General, in considering whether to proceed to give the technical capability notice, must have regard to the copy of the report.").
[16] Assistance and Access Act §§ 317ZN-317ZR.
[17] Assistance and Access Act §§ 317E(1)(j)(ii); 317G(5)(d)(ii); 317L(2)(c)(ii); 317T(3)(b).

include any law in effect punishable by three years or more in prison.[18] The Act contains no limitations on what countries it may be invoked on behalf of; there is neither a requirement that the foreign government provides for a minimum level of human rights protections nor that serious foreign crimes satisfy dual criminality with the criminal laws of Australia. This provision singularly amplifies the potential for negative consequences of the Act by several orders of magnitude. Without these provisions, Australia risks becoming the enabler of repressive and authoritarian regimes around the world.

Accepting a foreign country's threshold for a serious offense is dangerous. Doing so places the Australian government in a position not only to compromise rights and security of Australians, but also its international commitment to human rights if it foregoes its due diligence in deciding which governments get to use these powers and for which specific purposes.[19] For example, in the United Kingdom, it is a serious offense, punishable by several years in prison, to injure or kill a swan.[20] In fact, the European Union's attempts to establish a common legal framework for accessing electronic evidence continues to fail to bridge the differing legal standards across its member jurisdictions; this in spite of all the pre-existing treaties and agreements between EU's member states. Outside the EU there are even more significant risks. It is notable that India metes out life sentences for sedition crimes.[21] In Saudi Arabia, both homosexuality and witchcraft are crimes that are punishable with either significant prison time or with the death penalty.[22]

The same issues arise in the context of national security. Governments around the world invoke "national security" to justify mass intrusions into private data and interferences with the exercise of human rights.[23] The Council of Europe 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."[24]

Recommendations:

[18] Assistance and Access Act § 317B.
[19] *See*, *e.g.*, https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[20] *See* https://www.bbc.com/news/uk-wales-south-west-wales-39638665.
[21] *See* https://www.reuters.com/article/us-india-court-sedition/indian-opposition-seeks-scrapping-of-1870-sedition-law-after-students-charged-idUSKCN1PA13N.
[22] *See* https://www.theatlantic.com/international/archive/2013/08/saudi-arabias-war-on-witchcraft/278701/; https://www.independent.co.uk/news/world/middle-east/gay-saudi-arabian-man-sentenced-to-three-years-and-450-lashes-for-meeting-men-via-twitter-9628204.html.
[23] *See, e.g.,* http://news.bbc.co.uk/2/hi/sci/tech/1357513.stm; https://motherboard.vice.com/en_us/article/534pmd/how-an-illegal-canadian-spy-program-sailed-through-regulatory-checks-opc-odac-csis; https://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined ("National security (and other government interests) may justify some narrow intrusions on privacy in some circumstances. The problem with the programs disclosed over last week is that they are so astonishingly broad.").
[24] https://rm.coe.int/16806da51c at 16-17.

- In order to limit the Act's reach and to remove incentives for foreign manipulation of Australian officials, all provisions allowing for the Assistance and Access Act to be used to assist with serious foreign offences should be removed.[25]
- In the alternative, these provisions must be amended to refer to an "approved foreign government agency."
    - A definition for an approved foreign government agency should be then added, to denote a government agency that has applied for approval from the Home Affairs Office to request the use of these authorities and for which the Home Affairs Office has issued a public determination finding that the government agency meets a minimum standard for the protection of human rights, including through the presence of a framework for government surveillance that requires a judicial showing that surveillance is necessary and proportionate prior to its commission.
    - The Assistance and Access Act should mandate rejecting any application by a foreign government agency that does not meet this minimum standard, including any agency of a government that broadly criminalizes speech, including criticism against the government, or that discriminate on the basis of race, religion, national origin, sexual orientation, or other protected classes.
    - Parliament should further amend the Act to significantly increase the standard for what constitutes a serious foreign offense, including through the identification of an exclusive list enumerated categories of offenses that meet the qualification.
    - Annual reports should be mandated that include, at a minimum, a list of all approved foreign government agencies as well as a list of serious foreign offences for which the Assistance and Access Act has been requested to be used, as well as for which ones it was approved or denied.

Substantially limit the Act's potential to be used in harmful and dangerous ways by limiting the justifications and objectives for its use

The Assistance and Access Act fails to provide a level of clarity and precision sufficient to ensure that individuals have advanced notice of and can foresee its application. The ability to invoke its use not only for generic purposes, including "safeguarding national security" or "enforcing the criminal law,"[26] but also for matters that are "ancillary" or "incidental" to those objectives gives the Act nearly limitless scope that must be restricted and connected to greater transparency.[27] The ability for the Act to be used in ways that are ancillary and incidental should be removed in each instance within the Act to ensure it is applied in specific ways that could be anticipated.[28]

Moreover, the Assistance and Access Act also fails to embody the proper human rights standard of necessity and proportionality. Instead, the Act requires that authorities issuing

[25] Assistance and Access Act §§ 317G(5)(b); 317L(2)(c)(ii); 317T(3)(b).
[26] Assistance and Access Act §§ 317G(5)(a)-(d); 317L(2)(c); 317T(3)
[27] Assistance and Access Act §§ 317G(2)(a)(vi); 317G(2)(b)(vi); 317L(2)(d); 317T(2)(a)(ii).
[28] Necessary and Proportionate adequacy principle, see https://necessaryandproportionate.org/principles. *See also* discussion *supra* p. 4.

requests or notices are satisfied the requests or notices are "reasonable and proportionate."[29] Human rights law generally requires the "necessity" of an order, such that it is the only way to achieve an objective or the method that least risks human rights.[30] It is even more important for an assistance or capabilities be necessary when there is a high risk that doing so makes the platform less secure, and will expose users to subsequent security risks.

In order to reflect that standard, the factors that the relevant officer must regard must reflect considerations relevant to the specific objectives of the request as well as the human rights and security equities. As has been addressed in civil society and industry comments in the process of passing the Assistance and Access Act, the consequences of TARs, TANs, and TCNs will be global. The factors should therefore extend to the broader, international security implications of requests and orders.

The potential for abuse is particularly high in relation to TARs.[31] Entities that are non-consumer facing, including defense contractors and surveillance companies, have little incentive to push back against improper government requests. The extreme secrecy built into the Act exacerbates these equities by shielding these private entities from even the most basic levels of public accountability. It is at least partially for these reasons that we recommend removing the section authorising TARs from the Assistance and Access Act in its entirety (see more below). However, even if removal is unable to take place, the standards for TARs should be reviewed with even greater scrutiny and specifically limited to protect against overreach and abuse.

Recommendations:

- The standard for the issuance of TARs, TANs, and TCNs in the Act should be modified from "reasonable and proportionate" to "necessary and proportionate."
- The identified factors relevant to determining if this standard has been met should also be modified, with current factors being removed in exchange for more appropriate and representative elements, including:
    - (a) relevant objective identified by the [request/notice];
    - (b) impact on the designated communications provider, including any users or customers;
    - (c) availability of other means to achieve the objective;
    - (d) reasonableness of the acts or things sought;
    - (e) impact on persons other than the target of the [request/notice], including human rights impacts;
    - (f) human rights interests of the target, including rights to privacy and freedom of expression;
    - (g) potential or likely impact on domestic and international cybersecurity;

[29] Assistance and Access Act §§ 317JAA(1)(a), 317JAA(2)(a), 317JAA(3)(a), 317JAA(4)(a), 317JA(11)(a), 317JA(12)(a), 317JA(13)(a), 317JA(14)(a), 317JB(1A)(a), 317JB(2A)(a), 317JB(3A)(a), 317JB(5)(a), 317P(a), 317Q(10)(a), 317R(2)(a); 317R(4)(a), 317V(a), 317WA(7)(a)(ii), 317X(4)(a), and 317Z(2)(a).
[30] Necessary and Proportionate Principles, Necessity, *available at* https://necessaryandproportionate.org/principles#principle3.
[31] Assistance and Access Act §§ 317G(1)(c)-(d).

    - (h) potential or likely impact on Australia's digital economy and the international competitiveness of the designated communications provider.[32]
- Broad objectives contravene basic human rights principles. To prevent the invocation of broadly defined objectives that are more likely to lead to overreach and abuse, the Assistance and Access Act should require officials to indicate their intended objectives with specificity and to add transparency requirements to ensure that objectives are regularly reported to the public.[33] Specifically, Parliament should add a requirement for officials to detail a specific legal interest within the general objective (e.g., national security, serious Australian offenses) that the authority is being issued to achieve, as well as an explanation on how the acts or things sought relate to that objective.
- Potential relevant objectives for TARs should be limited to a specified list, enumerated within the Act.[34] Additionally, categories of relevant objectives should be substantially limited in order to prevent overreach, including removal of the objective relating to "the interests of Australia's foreign relations or the interests of Australia's national economic well-being."[35] Additionally, the objective referring to "matters relating to the security and integrity of information" should be modified to clarify that TARs should only be utilised in pursuit of improving "the security and integrity of information."[36]
- The sections creating TARs should be modified to require that TARs include the same duration limitations as TANs and TCNs, namely that the authority should include an expiry of no longer than one year.[37] A judicial review should happen at the time of renewal of all authorities to consider any change in circumstances, as well as information about how the authority has been utilised and any foreseen or unforeseen consequences. Additionally, the Act should be amended to add a procedure for designated communications provider to request revocation of a notice when material change in circumstances mean the standard is no longer satisfied. The request for revocation should be reviewed by a competent judicial authority in line with our above recommendations.

Other amendments necessary in order to ensure protection of human rights

The changes above represent only some of the most important changes that should be made to bring the Assistance and Access Act in compliance with international human rights law, protect Australians, and preserve digital security globally. Below are some of these additional changes that we recommend Parliament to consider.

Broad recommendations:

[32] Assistance and Access Act §§ 317JC, 317RA, 317ZAA.
[33] Examples may include objectives related to specific geographies or groups, specific crimes, or a specific mission. Objectives should be defined with the greatest granularity possible.
[34] Assistance and Access Act § 317G(5).
[35] Assistance and Access Act § 317G(5)(b).
[36] Assistance and Access Act § 317G(5)(c).
[37] Assistance and Access Act §§ 317MA(1A); 317TA(1A).

Notwithstanding any other recommendations in this submission, we urge Parliament to consider the following:

- It is prudent for Parliament to revisit the Assistance and Access Act outright and potentially to postpone its implementation by law until a full consideration of its potential impacts can be studied, including through the requirement for a more complete factual record justifying its necessity. At a minimum, implementation of the Act should be postponed until a full human rights impact assessment can be conducted. The assessment should analyse, among other things, what additional legal or policy protections are needed, including a comprehensive bill of rights or statutory protections for the pursuit or commission of activities that constitute government hacking.[38]
- While the explanatory materials associated with the Assistance and Access Act provide context on the distinction between TANs and TCNs, such distinction is largely absent from the Act itself.[39] As a result there are few provisions that limit TANs, which have fewer safeguards and limitations than TCNs, from being lawfully used in ways that it is theoretically meant to prevent. While it may be possible, and is definitely prudent, to remedy this deficiency through a series of changes, Parliament should instead consider removing TANs from the Assistance and Access Act outright, consolidating the authority into the provisions regarding TCNs. By doing so, Parliament will not only prevent unintended uses, but also facilitate much-needed clarity and consolidation in the Act's provisions.
- As explained in this submission,[40] the creation of TARs and the associated waiver of legal liability creates significant risks for corporate malfeasance and significant incentives for designated communications providers to pursue strategies of "over-compliance" in response to requests from government officials. To curb these risks, TARs should be stripped completely from the Assistance and Access Act. Instead, all government interventions seeking to compel certain acts or things from private industry actors must be subject to judicial review and strict safeguards.

Specific recommendations:

The following recommendations relate to specific provisions within the Act:[41]

- The broad definition of "acts or things" allows room for abuse and misuse, and must be limited to protect against the worst applications of the Act, including its use to erode vital security protections or to manipulate corporate employees to act outside of existing accountability mechanisms:

[38] *See* https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf. For a full accounting of the protections needed vis a vis government hacking, *see* https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf.

[39] *See* https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/ems/r6195_ems_b832c54b-6091-41ca-baf4-35bb94a856e8%22.

[40]

[41] In addition to these recommendations, we also offer by way of a technical fix that the use of "person" should be replaced by "designated communications provider". Assistance and Access Act §§ 317JB, 317R, and 317Z.

    - The most egregious provisions of the definition of "acts or things" should be removed to limit what designated communications providers can be requested or compelled to do.[42]
    - Provisions allowing acts or things to be required outside of the definition in the Act should be removed.[43] Additionally, throughout the Act, references to "acts or things" should be changed to refer instead to "listed acts or things."[44]

- The definitions of "systemic vulnerability" and systemic weakness" must be expanded, with the text referring to "a [vulnerability / weakness] that affects a whole class of technology," changed to "a [vulnerability / weakness] that has direct or foreseeable impacts outside of the target technology." It is also necessary to limit the definition of "target technology" to specify not only a "particular person" but "a particular individual who is relevant and material to pursuit of a relevant objective."[45]
- A provision should be included that extends the assessment that designated communications providers may request for TCNs to also apply to the issuance of TANs. Extend option for an assessment to TANs.[46]
- The assessment as provided for by the Assistance and Access Act highly preferences government interests over those of the general public and the designated communications provider.[47] To better represent all impacted parties, the process should be significantly amended.
    - Rather than rely upon two reviewers chosen by government officials, the Act should provide for a board or panel of assessors (an "Assessment Board"), which should include equitable representation of different backgrounds, including experts in privacy and cybersecurity. The Assessment Board should be authorised to review the full record and to issue a recommendation, with input from the government agency and the provider. Members of the Assessment Board should be appointed for a term of years and should be publicly identified.
    - Upon the issuance of a report from the Assessment Board, the Designated Communications Provider should be given an opportunity to issue a consenting or dissenting opinion. Any Assessment should always be without charge to the Provider.
    - The Assessment Board should be able to be called upon in advance of a Designated Communications Provider filing an appeal with a court of review of a judge's issuance of a TAN or TCN. In reaching its decision, the court of review should be required to consider the full record, including any report from an Assessment Board as well as any consenting or dissenting opinion submitted by the Designated Communications Provider.
- The Designated Communications Providers subject to Assistance and Access Act should be materially limited.

[42] Strike Assistance and Access Act §§ 317E(1)(a), 317E(1)(e)(1)-(2), 317E(1)(7), 317E(1)(f), 317E(1)(h), 317E(1)(j).
[43] Strike "(but are not limited to)," Assistance and Access Act §§ 317G(6), 317JA(10); strike Assistance and Access Act § 317JA(9); strike Assistance and Access Act §§ 317T(4)(c)(ii) and 317T(5)-(6).
[44] *See, e.g.*, Assistance and Access Act §§ 317K, 317G(1)(iv), 317L(1).
[45] Assistance and Access Act § 317B. Note, for this fix to be effective the approach to relevant objectives must also be modified as recommended herein.
[46] Assistance and Access Act §§ 317W; 317Y.
[47] *Id*.

- The definition of "Designated Communications Provider" should be amended to require a material connection to Australia.[48]
    - Categories of Designated Communications Providers that are tangential to the provision of eligible activities should be removed to protect against the opportunistic use of TARs, TANs, and TCNs.[49]
    - Non-executive level employees should be protected from being exploited by amending the definition of Designated Communications Provider to qualify that the scope "does not include a person who performs such services in the capacity of an employee of the provider."[50]
- The Assistance and Access Act should be amended to prevent against unnecessary interference with the right to freedom of expression and to provide for increased transparency.
    - The exception to the definition of acts or things that protects against compelled statements of fraud should be extended to also protect against compelled material omissions.[51]
    - In order to protect civil society and encourage robust public dialogue and accountability concerning the scope and use of the Assistance and Access Act, provisions prohibiting counseling against compliance with its provisions must be removed.[52]
    - Provisions establishing overbroad gag orders should be limited to facilitate public accountability and protect whistleblowers, who serve a vital role in government.[53]
    - All uses of TARs, TANs, and TCNs should be tracked and outcomes should be regularly reported. Statistics regarding the judicial approval, denial, or request for modification of TARs, TANs, and TCNs should be published at least semi-annually, along with identification of authorities seeking to invoke the authorities and the specific objectives being pursued that constitute legitimate government aims.[54]

Thank you for this opportunity to provide commentary and recommendations on your review of the Assistance and Access Act. We cannot overemphasize the importance of this inquiry and the need to amend the Act significantly to protect against disastrous impacts on human rights and digital security around the world.

If you have any questions or would like clarification on these recommendations, we are available for further consultation.

Thank you,

[48] Assistance and Access Act § 317C.
[49] Strike Assistance and Access Act §§ 317C(b)(5), (7), and (8).
[50] Assistance and Access Act § 317C. *See also* Assistance and Access Act § 317B (definition of "contracted service provider").
[51] Assistance and Access Act § 317E(2).
[52] Assistance and Access Act § 317E(2).
[53] Strike Assistance and Access Act § 317ZF. In the alternative, this section should be amended to add specific protections for whistleblowers who are protecting the public against waste, fraud, and/or abuse.
[54] These provisions should be added to Assistance and Access Act § 317ZS.

Amie Stepanovich
Global Policy Counsel
Access Now
[redacted]

Lucie Krahulcova
Asia Policy Analyst
Access Now
[redacted]

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
VIA email: pjcis@aph.gov.au and portal: www.aph.gov.au/pjcis

12 July 2019

Re: Review of the Amendments Made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

Introduction

Passed in December 2018, the Assistance and Access Act poses a grave risk to human rights and digital security around the world.[55] The Act should be fully repealed in order to ensure adequate time for a full reconsideration of the breadth and scope of its provisions, which did not happen prior to passage. Absent a repeal, the Act should be suspended for the duration of the current inquiry and/or until it is amended to limit the risks it currently poses, including risks to Australia's national security, information security and its digital economy. Herein we specifically recommend changes to improve human rights safeguards, including greater transparency, as well as to embody proper international human rights standards from the International Covenant on Civil and Political Rights (ICCPR) and other documents.

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[56] By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as

[55] Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, No. 148 (2018), *available at* https://www.legislation.gov.au/Details/C2018A00148. Hereinafter, "Assistance and Access Act" or "the Act."
[56] *See* https://www.accessnow.org/.

RightsCon, we fight for human rights in the digital age.[57] In 2018, Access Now published a report on "Human Rights in the Digital Era" evaluating Australia's role in the international community,[58] building on our earlier inputs to Australia's International Cyber Engagement Strategy in 2017.[59]

During its short legislative pendency, Access Now produced four submissions regarding early drafts of the Assistance and Access Act.[60] In September 2018, we commented to the Department of Home Affairs on the consultation draft, highlight its overbreadth and implications for digital security.[61] When the Act was introduced, mere weeks later, and without any response to the thousands of comments submitted, we submitted comments to the Joint Committee on Intelligence and Security, with specific recommendations to improve the proposal.[62] We also signed on to comments from a coalition of groups highlighting several deficiencies in the bill.[63]

Access Now followed up with another submission in November 2018, emphasizing the lack of factual record available in support of extraordinary powers contained in the bill, and imploring the Committee to delay its consideration until basic questions could be answered. [64] Finally, we made specific recommendations in February 2019 in order to support the development of amendments to the Act by providing the Committee with additional definitions, standards for judicial oversight and transparency requirements; all of which seek to mitigate the most detrimental impacts of the Act.[65]

The bill was ultimately pushed through passage in late December with only minimal changes and any discussion of amendments has been somewhat suppressed during the election period. We do note that the Committee supported two key amendments in the 2019 review:[66]

- bring forward the timeframe for the Independent National Security Legislation Monitor (INSLM) review of the Assistance and Access Act; and

[57] *See* https://www.accessnow.org/about-us/.
[58] *See* https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf.
[59] *See* https://www.accessnow.org/cyber-engagement-strategy-australia-overlooks-threats-user-rights/.
[60] Experts at Access Now were also invited to testify prior to the publication of a draft of the bill. *See*, accessnow.org/testimony-before-the-parliament-of-australia-parliamentary-joint-committee-on-law-enforcement/.
[61] accessnow.org/cms/assets/uploads/2018/09/Access-Now-Assistance-and-Access-Bill-submission.pdf.
[62] *See* https://www.accessnow.org/cms/assets/uploads/2019/02/Sub33.pdf.
[63] *See* https://www.efa.org.au/main/wp-content/uploads/2018/10/Submission-Assistance-and-Access-Bill-2018_collaborative_submission.pdf, https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Comments_on_Australia_Assistance_and_Access_Bill_2018_10-11-18.pdf, https://www.commsalliance.com.au/Documents/releases/2016-media-releases3/2018-media-release-27, https://newamericadotorg.s3.amazonaws.com/documents/Coalition_comments_on_Australia_bill.pdf. *See also* https://www.efa.org.au/main/wp-content/uploads/2018/07/Australia-Encryption-Coalition-Letter.pdf.
[64] *See* https://www.accessnow.org/cms/assets/uploads/2019/02/Sub33.1-2.pdf.
[65] Not yet available online.
[66] https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024269/toc_pdf/ReviewoftheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf

- extend industry assistance powers provided for in the Act to Commonwealth and state anti-corruption bodies.[67]

We remain committed to supporting the work of the Parliamentary Joint Committee on Intelligence and Security as they continue to investigate and evaluate the impact of this legislation alongside the Independent National Security Legislation Monitor, and will be following the developments in 2020 when the Parliamentary inquiry as well as the independent report are due. We hope that the Committee will take any opportunity to, at a minimum, remedy the most egregious parts of the grossly overbroad Act.

We will limit the below comments to the scope foreseen in the terms of reference and the current round of inquiry.[68] However, the below comments are complementary and should be interpreted alongside the previous comments Access Now submitted to the Committee.

Key Issues

1. Lack of safeguards for protecting the rights of individuals

The Act violates human rights law by failing to require judicial approval

International human rights law requires that "determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent."[69] As pointed out by the Australian Human Rights Commission (HRC), despite this international recognition of the vital role of an independent and impartial judiciary in overseeing the application of counter-terrorism laws, new counter-terrorism powers tend to be located in the executive, rather than the judicial branch, of government.[70] In its assessment, the HRC warns that the legal test must not only take place - it must provide for a meaningful and informed application - which they reference to the National Security Information Act of 2004.[71] Similar issues and warnings echo to the Assistance and Access Act, "the executive arm of government should be wary of exercising decision-making powers in circumstances which appear to 'trump' decisions of the judiciary."[72]

---

[67] Noting from the Parliamentary report from April 2019 that;"The committee is therefore of the view that the Commonwealth Ombudsman should oversight the use of these powers by state bodies. Such an extension is parallel with the Ombudsman's oversight of the exercise of the act's powers by state and territory police forces."

[68] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Terms_of_Reference .

[69] Necessary and Proportionate Principles, Competent Judicial Authority, *available at* https://necessaryandproportionate.org/principles#principle6.

[70] Hon John Von Doussa QC, 'Incorporating Human Rights Principles into National Security Measures', Australian Human Rights Commission, https://www.humanrights.gov.au/about/news/speeches/incorporating-human-rights-principles-national-security-measures

[71] Hon Michael McHugh AC QC, 'Terrorism Legislation and the Constitution' (2006) 28 Australian Bar Review 117.

[72] Hon John Von Doussa QC, 'Incorporating Human Rights Principles into National Security Measures', Australian Human Rights Commission,

It is beyond question that the Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) created by the Assistance and Access Act relate to communications surveillance, most directly by facilitating its commission. However, the provisions of the Assistance and Access Act that create these authorities do not require judicial approval, or even judicial involvement.[73] The consequence is that government officials with the authority to issue TANs and TCNs are given nearly unchecked power to unilaterally approve invasive activities with unpredictable and potentially dangerous outcomes.[74]

Moreover, the Act fails to provide adequate right to a legal appeal. Taken together, this means there is very limited opportunity to challenge the lawfulness of a TAN or TCN.[75] Even worse is that the Act contains provisions for the delegation of authority to issue TANs and TCNs to an even greater number of officials, compounding the probability that the Act will be misused or used in ways that have severe unexpected or unintended consequences.

Transparency is necessary to ensure accountability

In order for individuals to exercise their rights, it is essential that the Government's use of the Act -- and the extent of such usage -- is communicated clearly and publicly. Without transparency and adequate review mechanisms, there are no safeguards to protect individuals from the injustice that would result from the abuse, misuse, or erroneous application of the counter-terrorism powers. In their assessment of incorporating human rights into counter-terrorism legislation, HRC points out that "ensuring compatibility with human rights improved transparency and parliament accountability." They further added that, "a permanent independent reviewer should be given powers to gather information from a wide range of sources, including intelligence agencies; and be required to consider the human rights impacts of the laws."[76]

All uses of TARs, TANs, and TCNs should be tracked and outcomes should be regularly reported. Statistics regarding the judicial approval, denial, or request for modification of

---

https://www.humanrights.gov.au/about/news/speeches/incorporating-human-rights-principles-national-security-measures

[73] The use of the authorities would only involve a judge when used in connection with an existing authority with a requirement for judicial approval, though the approval would be limited to the utilisation of that authority. Conversely, all other uses would be unilaterally authorised and exercised.

[74] Assistance and Access Act § 317L(1) ("The Director-General of Security or the chief officer of an interception agency may give a designated communications provider a notice, to be known as a technical assistance notice, that requires the provider to do one or more specified acts or things..."); Assistance and Access Act 317T(1) ("The Attorney-General may, in accordance with a request made by the Director-General of Security or the chief officer of an interception agency, give a designated communications provider a written notice, to be known as a technical capability notice, that requires the provider to do one or more specified acts or things").

[75] In regard to TCNs, the provider may request an assessment, but the scope of that assessment is limited, as is its ability to impact the final decision to compel the provider to act. *See* Assistance and Access Act § 317WA. ("If a consultation notice is given to a designated communications provider under subsection 317W(1) in relation to a proposed technical capability notice, the provider may, within the time limit specified in the consultation notice, give the Attorney-General a written notice requesting the carrying out of an assessment of whether the proposed technical capability notice should be given."; "the Attorney-General, in considering whether to proceed to give the technical capability notice, must have regard to the copy of the report.").

[76] Hon John Von Doussa QC, 'Incorporating Human Rights Principles into National Security Measures', Australian Human Rights Commission, https://www.humanrights.gov.au/about/news/speeches/incorporating-human-rights-principles-national-security-measures.

TARs, TANs, and TCNs should be published at least semi-annually, along with identification of authorities seeking to invoke the authorities and the specific objectives being pursued that constitute legitimate government aims.[77]

Recommendations

- The Assistance and Access Act must be amended to require all TANs and TCNS to be approved and issued by a competent judicial authority who is impartial and independent. The judge should have the authority to examine the full scope of an application and to issue a ruling both regarding the extent it meets the requirements of the Act for containing the proper elements, including a specifically identified objective, as well as if it satisfies the standard for the notice to issue.
- Parliament must add new provisions to provide designated communications providers a right to appeal any TAN or TCN to a court of review if they believe that the judge who issued the authority applied the standard improperly.
- Involvement of a judge should extend beyond issuance of notices to also include extensions, variances, renewals, as well as any request for the designated communications provider for a notice to be revoked on the basis of a material change in circumstances that impacts its development or use.
- Provisions allowing delegation of issuance of TANs and TCNs, as well as Technical Capability Requests (TARs), should be removed. In the alternative, delegation must be limited to only the most senior officials and only in limited, enumerated circumstances.[78] Special accountability mechanisms should be included to track delegations and publish information on the use of TARs, TANs, and TCNs by delegated officials.

2. Inconsistency with necessary and proportionate legal standards

As we have previously iterated in our submissions, the Assistance and Access Act also fails to embody the proper human rights standards of necessity and proportionality. Instead, the Act requires that authorities issuing requests or notices are satisfied the requests or notices are "reasonable and proportionate."[79] International human rights law provides a carefully calibrated set of indicators which enable governments to balance national security and human rights. It provides that states may take protective action which limit derogable human rights in carefully refined circumstances, as set out in Article 4 of the ICCPR, "[acts] that may be justifiable infringed by States in times of public emergency which threatens the life of the nation."[80]

[77] These provisions should be added to Assistance and Access Act § 317ZS.
[78] Assistance and Access Act §§ 317ZN-317ZR.
[79] Assistance and Access Act §§ 317JAA(1)(a), 317JAA(2)(a), 317JAA(3)(a), 317JAA(4)(a), 317JA(11)(a), 317JA(12)(a), 317JA(13)(a), 317JA(14)(a), 317JB(1A)(a), 317JB(2A)(a), 317JB(3A)(a), 317JB(5)(a), 317P(a), 317Q(10)(a), 317R(2)(a); 317R(4)(a), 317V(a), 317WA(7)(a)(ii), 317X(4)(a), and 317Z(2)(a).
[80] In order for States to derogate from their obligations under article 4 of the ICCPR in times of public emergency, art 4(1) provides that; the public emergency must threaten the life of the nation; the public emergency must be publicly proclaimed; the measures must be strictly required by the exigencies of the situation; the measures cannot be inconsistent with other requirements of international law; and the measures must not involve

However, any such restrictions on rights to privacy and expression are subject to a "permissible limitations" test.[81] Pursuant to UN Human Rights Committee General Comment Number 34 on Article 19 of the ICCPR, such "permissible" restrictions must be provided by law; strictly serve a legitimate aim (respect of the rights and reputation of others, protection of national security or of public order, or of public morals or health); and meet a high standard of legality, proportionality, and necessity. Human rights law therefore requires the "necessity" of an order, such that it is the only way to achieve an objective or the method that least risks human rights.[82] It is even more important for an assistance or capabilities notice to satisfy that standard when there is a high risk that doing so makes the platform less secure, and will expose users to subsequent security risks. As stated on the Attorney-General's website under Permissible limitations to Human Rights, any such legislation must be assessed against the following questions to determine if limiting human rights in such an instance is reasonable, necessary and proportionate:[83]

- Will the limitation in fact lead to a reduction of that problem?
- Does a less restrictive alternative exist, and has it been tried?
- Is it a blanket limitation or is there sufficient flexibility to treat different cases differently?
- Has sufficient regard been paid to the rights and interests of those affected?
- Do safeguards exist against error or abuse?
- Does the limitation destroy the very essence of the right at issue?

The current round of inquiry by the PJCIS should yield answers to these questions, still, given the nature and scope of the impact that the measures contained in the Assistance and Access Act are likely to have -- the Act as it stands should be repealed or suspended until such a time -- and until substantial amendments are agreed upon.

Furthermore, the International Principles on the Application of Human Rights to Communications Surveillance say, "privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognized under international human rights law."[84]

---

discrimination solely on the grounds of race, sex, colour, language, religion or social origin. Art 4(2) of the ICCPR mandates that certain rights are not subject to suspension under any circumstances. The list of non-derogable rights includes the right to life (article 6); freedom of thought, conscience and religion (article 18); freedom from torture or cruel, inhuman or degrading punishment or treatment (article 7); the right to recognition everywhere as a person before the law (article 16) and the principles of precision and non-retroactivity of criminal law (article 15). August 2001 the Human Rights Committee adopted a list of elements that, in addition to the rights specified in article 4(2), cannot be subject to lawful derogation: https://www.refworld.org/docid/453883fd1f.html.

[81] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/ HRC/23/40 ¶¶ 28, 29 (Apr. 17, 2013) by Frank La Rue.

[82] Necessary and Proportionate Principles, Necessity, *available at* https://necessaryandproportionate.org/principles#principle3.

[83] Attorney-General's Department, Permissible limitations to Human Rights: https://www.ag.gov.au/RightsAndProtections/HumanRights/Human-rights-scrutiny/PublicSectorGuidanceSheets/Pages/Permissiblelimitations.aspx .

[84] International Principles on the Application of Human Rights to Communications Surveillance (May 2014), https://necessaryandproportionate.org/text [hereinafter "Necessary and Proportionate Principles"].

In order to reflect these standards, the factors that the relevant officer must regard must reflect considerations relevant to the specific objectives of the request as well as the human rights and security equities. As has been addressed in civil society and industry comments in the process of passing the Assistance and Access Act, the consequences of TARs, TANs, and TCNs will be global. The factors should therefore extend to the broader implications that requests and orders are likely to have on the security of the digital infrastructure that we all share.

The potential for abuse is particularly high in relation to TARs.[85] Entities that are non-consumer facing, including defense contractors and surveillance companies, have little incentive to push back against improper government requests. The extreme secrecy built into the Act exacerbates these equities by shielding these private entities from even the most basic levels of public accountability. It is at least partially for these reasons that in our previous submission we have recommended removing the section authorising TARs from the Assistance and Access Act in its entirety. However, even if removal is unable to take place, the standards for TARs should be reviewed with even greater scrutiny and specifically limited to protect against overreach and abuse.

Recommendations

- The standard for the issuance of TARs, TANs, and TCNs in the Act should be modified from "reasonable and proportionate" to "necessary and proportionate."
- The identified factors relevant to determining if this standard has been met should also be modified, with current factors being removed in exchange for more appropriate and representative elements, including:
    - (a) relevant objective identified by the [request/notice];
    - (b) impact on the designated communications provider, including any users or customers;
    - (c) availability of other means to achieve the objective;
    - (d) reasonableness of the acts or things sought;
    - (e) impact on persons other than the target of the [request/notice], including human rights impacts;
    - (f) human rights interests of the target, including rights to privacy and freedom of expression;
    - (g) potential or likely impact on domestic and international cybersecurity;
    - (h) potential or likely impact on Australia's digital economy and the international competitiveness of the designated communications provider.[86]
- Broad objectives contravene basic human rights principles. To prevent the invocation of broadly defined objectives that are more likely to lead to overreach and abuse, the Assistance and Access Act should require officials to indicate their intended objectives with specificity and to add transparency requirements to ensure that objectives are regularly reported to the public.[87] Specifically, Parliament should add a requirement for officials to detail a specific legal interest within the general

[85] Assistance and Access Act §§ 317G(1)(c)-(d).
[86] Assistance and Access Act §§ 317JC, 317RA, 317ZAA.
[87] Examples may include objectives related to specific geographies or groups, specific crimes, or a specific mission. Objectives should be defined with the greatest granularity possible.

objective (e.g., national security, serious Australian offenses) that the authority is being issued to achieve, as well as an explanation on how the acts or things sought relate to that objective.

- Potential relevant objectives for TARs should be limited to a specified list, enumerated within the Act.[88] Additionally, categories of relevant objectives should be substantially limited in order to prevent overreach, including removal of the objective relating to "the interests of Australia's foreign relations or the interests of Australia's national economic well-being."[89] Additionally, the objective referring to "matters relating to the security and integrity of information" should be modified to clarify that TARs should only be utilised in pursuit of improving "the security and integrity of information."[90]
- The sections creating TARs should be modified to require that TARs include the same duration limitations as TANs and TCNs, namely that the authority should include an expiry of no longer than one year.[91] A judicial review should happen at the time of renewal of all authorities to consider any change in circumstances, as well as information about how the authority has been utilised and any foreseen or unforeseen consequences. Additionally, the Act should be amended to add a procedure for designated communications provider to request revocation of a notice when material change in circumstances mean the standard is no longer satisfied. The request for revocation should be reviewed by a competent judicial authority in line with our above recommendations.

Contact

Thank you for this opportunity to provide commentary and recommendations on your review of the Assistance and Access Act. We cannot overemphasize the importance of this inquiry and the need to repeal or suspend the Act until it is significantly amended to protect against disastrous impacts on human rights and digital security around the world.

If you have any questions or would like clarification on these recommendations, we are available for further consultation. This submission was prepared with the support of Amie Stepanovic, U.S. Policy Manager and Global Policy Counsel at Access Now.

Thank you,

Lucie Krahulcova
Policy Analyst, Australia and Asia Pacific
Access Now
[redacted]

Raman Jit Singh Chima
Asia Policy Director and Senior International Counsel
Access Now
[redacted]

[88] Assistance and Access Act § 317G(5).
[89] Assistance and Access Act § 317G(5)(b).
[90] Assistance and Access Act § 317G(5)(c).
[91] Assistance and Access Act §§ 317MA(1A); 317TA(1A).