July 11, 2019

RE: International Civil Liberties and Technology Coalition Comments Regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the amendments made to Commonwealth Legislation by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

To whom it may concern:

The undersigned organizations and companies jointly submit these comments regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the amendments made to Commonwealth Legislation by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 that was enacted in December 2018.[1] The threats to the rights of Australians arising from this Act are so severe that Australian civil society organizations have joined with an international coalition of civil society organizations dedicated to protecting civil liberties, human rights, and innovation online, as well as technology companies and trade associations, all of whom share a commitment to strong encryption and cybersecurity. We submit these comments to explain our continued concerns regarding the serious threats that this legislation poses to cybersecurity, privacy and freedom of expression. Indeed, while these threats are dire enough for Australians alone, they have similar implications worldwide. The broad new powers conferred by the Act to demand that tech companies weaken the security features of their products will affect all users of those products, wherever they are located. Protections for privacy, data security, and free expression that are derived from the availability of strong encryption would be undermined by government demands that communications providers introduce intentional vulnerabilities into secure products for the government's use.

The undersigned organizations and companies are part of a coalition that previously outlined the threats posed by earlier versions of this legislation in comments submitted in September, 2018[2] and October, 2018.[3] Many of us submitted another set of coalition comments on November 21, 2018, in a response to an invitation from the Parliamentary Joint Committee on Intelligence and Security (PJCIS),[4] as well as comments in February, 2019[5] focusing on the

[1] Our comments focus on Schedule 1 (Industry Assistance) except with regard to the discussion of the interaction with the intelligence agencies' other powers.
[2] *Coalition comments in response to the Exposure Draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Assistance and Access Bill)*, (Sept. 9, 2018), https://newamericadotorg.s3.amazonaws.com/documents/Coalition_comments_on_Australia_bill.pdf.
[3] *Coalition comments regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018*, (Oct. 11, 2018), https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Comments_on_Australia_Assistance_and_Access_Bill_2018_10-11-18.pdf.
[4] *Supplemental coalition comments regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018*, (Nov. 21, 2018),

amendments offered at the end of last year. We appreciate the Committee's work to review prior submissions, and the careful analysis of the last round of comments – including those from our coalition.[6] We also appreciate the development of areas of focus for further discussion, and this opportunity to reiterate our concerns and further discuss these themes.

Although we continue to oppose the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, now that the Act has passed and Parliament is conducting a mandatory review of the new legislation, we continue our call for amendments that would mitigate the threats to cybersecurity and human rights that the law poses. In light of this new call for comment, the undersigned organizations wish to emphasize the impact the Act will have on cybersecurity, privacy, and freedom of expression, but also highlight the conflicts the Act may create between Australian law and foreign laws, and the damage it may cause to Australian industry and competitiveness. The undersigned organizations urge Parliament to consider our recommendations, and make necessary changes so that the Act will do the least harm possible. These changes would ameliorate, though not cure, some of the most significant concerns the legislation now raises. Specifically, we urge that:

- The government should narrow the scope of the Act's powers by clarifying definitions of "systemic vulnerability" and "systemic weakness" and clarify that providers cannot be required to decrypt or ensure the ability to decrypt user communications.
- The Act should provide robust authorization processes with clear decision-making criteria, including requiring that a Federal court reviews all TCNs or TANs, and giving recipients the right to appeal these notices in order to create better oversight mechanisms.
- The government should narrow the scope of enforcement provisions by narrowing the definition in the law for "designated communications providers."
- Unless the Assistance and Access Act 2018 is repealed or significantly amended, it would significantly expand the authority of Australia's intelligence agencies by granting them unprecedented powers without adequate oversight.
- Unless the Assistance and Access Act 2018 is repealed or significantly amended, it imperils Australia's ability to qualify for a bilateral agreement under the U.S CLOUD Act.

---

https://newamericadotorg.s3.amazonaws.com/documents/Australia_supplemental_comments_Nov_21_2018.pdf.

[5] *Coalition comments regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018*, (Feb. 21, 2019), https://newamericadotorg.s3.amazonaws.com/documents/Coalition_comments_Australia_Assistance_and_Access_Law_2018_Feb_21_2019.pdf.

[6] *Committee Report regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018*, (April 2019), https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024269/toc_pdf/ReviewoftheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf.

- The Act, as enacted, will have a significant negative impact on Australian industry and competitiveness.
- The Act should be amended to provide for public oversight with additional reporting requirements, including mandatory annual reviews with a publicly-available summary.

## IMPORTANCE OF ENCRYPTION

Strong encryption is the cornerstone of the modern information economy's security. Encryption protects billions of people every day against countless threats—be they street criminals trying to steal our phones and laptops, computer criminals trying to defraud us, corporate spies trying to obtain our companies' most valuable trade secrets, or repressive governments trying to stifle dissent. Encryption thereby protects us from innumerable criminal and national security threats. These protections are not only for citizens alone; encryption protects the government itself from attacks by criminals, other governments, and data thieves the world over. Compromising encryption compromises all Australians individually and as a nation.

Additionally, encryption is essential to the rights of privacy and free expression. David Kaye, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, recommended in his 2015 report that states promote encryption and anonymity, noting that they "facilitate and often enable the rights to freedom of opinion and expression."[7] In his follow-up report in 2018, Kaye raised concerns that the technical capability notices authorised under the United Kingdom's Investigatory Powers Act could threaten encryption, and thus freedom of expression, and he noted Australia's intention to model this approach as "troubling."[8] Protections for privacy, data security, and free expression that are derived from the availability of strong encryption would be undermined by government demands that communications providers introduce intentional vulnerabilities into secure products for the government's use. Joseph Cannataci, United Nations Special Rapporteur on the right to privacy, submitted his own comments in a previous round of this process, saying that the Act "is an example of a poorly conceived national security measure that is equally as likely to endanger security as not; it is technologically questionable if it can achieve its aims...and it unduly undermines human rights including the right to privacy."[9]

---

[7] David Kaye, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report on the use of Encryption and Anonymity in Digital Communications (May 22, 2015), paragraphs 59-60, available at https://undocs.org/A/73/348.
[8] David Kaye, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Encryption and Anonymity Follow-up Report, (June 2018), 6, available at https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf.
[9] Joseph Cannataci, United Nations Special Rapporteur on the right to privacy, Letter regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018 (Oct. 12, 2018), 4, available at https://www.ohchr.org/Documents/Issues/privacy/O_LAUS_6.2018.pdf.

## AREAS OF FOCUS

### Threshold, Scope, and Proportionality of Powers

The Assistance and Access Act gives the Australian government overly-broad powers that create risks to device security and cybersecurity more generally. To protect the rights of Australians and users of technology around the globe, the law's scope should be significantly narrowed and the new powers must be reined in to be proportional.

First, the definitions of "systemic vulnerability" and "systemic weakness" are still not clear and specific enough to fully address our concerns about ambiguity or to sufficiently narrow the overly broad scope of powers granted to the Australian government. We renew our recommendation that these definitions should clarify that systemic vulnerabilities or weaknesses mean any vulnerability or weakness that could or would extend beyond the specifically targeted device or service that the targeted individual is using and is implemented in such a way that any other user of the same device or service, or any other device or service of the Designated Communications Provider, could or would be affected. In his comments in September, Special Rapporteur David Kaye expressed concern that "the draft Bill gives virtually unfettered discretion to agencies to compel providers to modify digital security standards or take other action that would effectively weaken encryption."[10]

The law should also make clear that the government is not authorized to require a designated communications provider to build or implement specific designs of equipment or services to decrypt communications; and that the government may not prohibit a designated communications provider from adopting any specific equipment or feature. As discussed further in the Industry Competitiveness section below, the broad scope of the government powers currently granted under the Act poses direct threats to Australian business and interests abroad. The law should also make clear that designated communications providers will not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication that has been encrypted by another individual or entity that uses the provider's product or service. If the user applied the encryption themselves, the Act must not make communications providers responsible for providing a way to decrypt that content.

### Authorization Processes and Decision-making Criteria

The law also lacks sufficiently robust authorization processes or clear decision-making criteria that will safeguard the digital rights of Australians and technology users around the globe.

[10] David Kaye, United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Letter regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018, (Sept. 11, 2018), 2, available at https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-AUS-5-2018.pdf.

Review by the Court (rather than approval by two Ministers) is necessary to ensure an independent, apolitical application of the law procedurally, and more importantly, an assessment of the validity of both the merits and objections to the application, or in this case Notice, before it is served on a designated communications provider. The law should be amended to establish a new section requiring that the Federal Court review and approve any technical assistance notice or technical capability notice issued by the government before it may be given to a designated communications provider. The criteria for this review should include an assessment of whether issuance of a relevant notice is correct; whether the relevant notice complies with the law and regulations prescribed, including the provisions in Section 317ZG (pp. 84-85) and Section 317ZH (pp. 87-90); whether the requirements imposed by the relevant notice are reasonable and proportionate; whether compliance with the relevant notice is practicable and technically feasible; whether compliance with the relevant notice would require a designated communications provider to violate the laws of a foreign jurisdiction; and whether the relevant notice serves a relevant objective.

At a minimum, Sections 317WA (pp. 56-60) and 317YA (pp. 64-48), should be expanded to cover challenges to technical assistance notices and amended to provide for review by the Federal Court following the issuance of the assessors' report and the Attorney-General's decision. If the report of the assessors raises significant concerns regarding the proposed technical assistance notice or technical capability notice, the Attorney-General should be required to seek review by the Federal Court before it can give such notice. The Federal Court would then be required to review whether the government's interest in giving the notice is so great that it significantly outweighs the concerns raised in the report of the assessment.

The law should also be amended to establish a right to appeal the issuance of a technical assistance notice or a technical capability notice, as well as a clear process for initiating that appeal, and a robust standard of review for the court to follow. As our coalition noted in previous comments, Section 317ZFA (pp. 83-84) of the law would explicitly confer jurisdiction on courts to "make such orders as the court considers appropriate in relation to the disclosure, protection, storage, handling or destruction" regarding information in connection with technical assistance requests, technical assistance notices, and technical capability notices. However, the law does not currently set forth any procedure to follow in challenging a technical assistance request, technical assistance notice, or technical capability notice, nor does it provide a clear and meaningful standard for a court to follow in reviewing such a challenge. Rather, Section 317ZFA (pp. 83-84) simply states that a court has the authority to issue appropriate orders "if the court is satisfied that it is in the public interest to make such orders," and the Explanatory Memorandum released with the bill in September states that these notices are not subject to a merits review (pp. 15, 29, 60). The fact that the law permits executive decision makers to issue expansive notices — impacting the privacy of individuals — without the added protections to test those decisions with full merits review at the judicial level, is particularly concerning. Moreover, given the law's strict non-disclosure provisions as outlined below, "affected persons" will never know that a notice has been issued. Thus, even if companies receiving a notice might be able to challenge the demand as unlawful, the actual "affected persons" would not be able to do so.

New Sections 317WA (pp. 56-60) and 317YA (pp. 64-48) create procedures through which providers may seek an assessment by a panel of "assessors" of whether a technical capability notice should be given or varied, and one of the assessors must be a former judge. Although this enhanced review process enables providers to initiate a challenge on their own, the inclusion of former judges as assessors does not convert this process into independent judicial review. This assessment process simply requires the preparation, delivery, and consideration of a report on whether a technical capability notice should be given or varied. More specifically, Subsection (6) of Sections 317WA and 317YA requires that the assessors must prepare a report containing their assessment and deliver that report to relevant government officials and the particular designated communications provider. Subsection (11) requires that the Attorney-General must "have regard to the copy of the report" when deciding whether to give or vary the technical capability notice. But there is no requirement that the Attorney-General follow the recommendation in the report, nor is there any provision for judicial review of the Attorney-General's decision.

Moreover, this new challenge procedure only applies to technical capability notices and not to technical assistance notices, even though technical assistance notices may be used to require providers to do "acts or things" including installing software and "removing one or more forms of electronic protection" that the provider had applied (Sec. 317E(1), p. 18). As we noted in previous comments, given the breadth and power of the new authorities this law would create, it is critical that the law provide for robust independent oversight of authorising agencies to ensure accountability.

**Scope of Enforcement Provisions**

The definition in the law for "designated communications providers" is overly broad. As our coalition noted in previous submissions, the current definition could affect hundreds of thousands, if not millions, of individuals in Australia and around the world. The Explanatory Memorandum explains that under this law, "designated communications provider" would apply to "the full range of participants in the global communications supply chain, from carriers to over-the-top messaging providers" (p. 35), and under the law this includes anyone who "provides an electronic service that has one or more end-users in Australia" (Sec. 317C, p. 15). Under the Explanatory Memorandum, "electronic service" is also broadly defined, and "may include websites and chat for secure messaging applications, hosting services including cloud and web hosting, peer-to-peer sharing platforms and email distribution lists, and others" (p. 37). These criteria also apply globally, since the law makes clear that the orders can be served outside Australia (Sec. 317ZL, pp. 99-101).

To address these concerns, the law should be further amended to limit entities that can be subject to technical assistance notices and technical capability notices to those that receive revenue from within Australia. Additionally, the definition of "designated communications provider" should be narrowed to exempt entities that do not have ongoing relationships with

users, such as software developers that publish software without operating associated services; entities that, for technical reasons, cannot identify an individual user within the context of their existing architecture; entities that are foreign governments; natural persons who are not acting on behalf of a corporate entity; and entities that only operate or maintain internet infrastructure such as underseas fiber optic cables.

**Interaction with Intelligence Agencies' Other Powers**

The Act would significantly expand the authority of Australia's intelligence agencies by granting them power to take aggressive action at their own discretion without formal supervision. The Director-General of Security (the head of ASIO), the Director‑General of the Australian Secret Intelligence Service, the Director‑General of the Australian Signals Directorate are each able to request designated communications providers to do a broad range of 'acts or things' on a voluntary basis, and the Director General of Security has been given power to compel the designated communications providers to do wide range of 'acts or things.'

The powers are broad because they can be exercised at the discretion of the head of the agency if they are directed towards safeguarding national security (in the case of ASIO), the interests of Australia's national security or its foreign relation interests (in the case of ASIS), and/or providing material and advice on matters relating to the security and integrity of information that is processed/stored/communicated by electronic means (re: the Australian Signals Directorate).

The immunity granted to national security agencies for use of TARs, TANs, and TCNs is also intentionally wider than the immunity that they have for other activities authorised by pre-existing legislation. Section 21A, which confers civil immunities on persons who voluntarily assist ASIO, lacks limitations on scope of, and issuing thresholds for, such immunities and its procedural provisions. It appears that the provision could be used to circumvent existing warrant requirements, and be used interchangeably with technical assistance requests. The Department rejected submissions by the IGIS along these lines.

The broad discretion with which the powers can be exercised gives rise to significant oversight and accountability concerns set out in detail by the Inspector General of Intelligence and Security (IGIS) in its submission to the PJCIS. These concerns were tempered somewhat through the introduction of limited reporting/notification requirements before the final Act was passed but have not been eliminated. These powers still lack standard reporting and notification obligations for when they are used to compel assistance and confer civil immunities. The IGIS considered that such requirements should have been included to ensure that oversight resources could be targeted properly and would be in line with existing reporting requirements for similarly intrusive powers.

Section 34AAA confers a coercive power on ASIO under which the Attorney-General can issue an order requiring certain persons to assist ASIO in accessing data seized under a warrant. The

IGIS commented adversely on this new power noting that the power is ambiguous and lacking safeguards. The provision appears to authorise deprivation of liberty and/or inhumane treatment. The government rejected a call from the IGIS for conditions and safeguards to be applied.

ASIO has a broad power to use force in the discharge of a computer access warrant issued under the ASIO Act 1979: Section 25A (5A) provides "A computer access warrant must… authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant…." The Act has expanded this authorisation to use force by allowing a computer access warrant to be issued for the purpose of intercepting a communication passing over a telecommunications system.

**Interaction with Foreign Laws, Including the United States' CLOUD Act**

The United States' Clarifying Lawful Overseas Use of Data Act (CLOUD Act) permits a qualifying country to enter into a bilateral agreement with the United States, which then enables the qualifying country to bypass the cumbersome, but rights-protective, Mutual Legal Assistance Treaty (MLAT) process and directly serve electronic evidence requests to a U.S.-based service provider. The CLOUD Act, which many of the undersigned organizations opposed, carries substantial privacy risks if countries seeking agreements lack appropriate constraints on government access to data and sufficient protections for individuals. We continue to urge that any bilateral agreements under the Act should incorporate additional safeguards for fundamental human rights beyond the minimum CLOUD Act requirements. The CLOUD Act is an important consideration in connection with the Assistance and Access Act 2018, because Australia's new law imperils Australia's ability to qualify for a bilateral agreement under the CLOUD Act.

In order for a country to qualify for a bilateral agreement, that country's laws must afford "robust substantive and procedural protections for privacy and civil liberties in light of data collection and activities of the foreign government that will be subject to the agreement" (§ 2523(b)(1)). Once the U.S. Attorney General certifies a negotiated bilateral agreement, that agreement must be submitted to the U.S. Congress. The CLOUD Act provides that Congress has 180 days to review the agreement, during which time Congress may vote to disapprove it. Due to Australia's enactment of the Assistance and Access Act of 2018, three of these CLOUD Act criteria may pose challenges to Australia's ability to qualify for a bilateral agreement through this process, namely criteria requiring (1) adherence to human rights obligations; (2) clear legal mandates, procedures, and oversight of agencies in how they access, use, and share the data; and (3) sufficient mechanisms to provide accountability and appropriate transparency with the collection and use of electronic data.

First, the Assistance and Access Act 2018 threatens digital rights, which are critical to safeguarding human rights. Encryption is essential to protecting the human rights of privacy and free expression, but with Australia's new Assistance and Access Act of 2018 undermining digital

security, the risks and threats to these human rights increase dramatically. The law imperils security protections that dissidents, human rights activists, and others rely on, and is particularly a risk for journalists who need to ensure the security of their sources.[11] In addition, the vast new powers that the law provides to the Australian government may have an adverse effect on the level of trust in otherwise secure communication systems. Users may no longer have confidence that they are communicating privately, or that they are speaking to the intended party or parties. By posing a threat to encryption, the law is likely to have a chilling effect upon speech.

Second, the lack of judicial or independent review and the broad discretion given to security agencies also raises concerns. Even the post-issuance review afforded by the Australia law is insufficiently robust, since there is no independent review or oversight of TCNs and TANs unless a provider files a challenge. Further, there can be no meaningful independent review or oversight if the sitting court or authority lacks a clear and robust standard of review to rely on when evaluating the lawfulness of a notice. The standard for issuing a TAN[12] or TCN[13] is simply that it must be "reasonable and proportionate" and that compliance with the notice must be "practicable and technically feasible." Although a government official is required to account for some considerations like legitimate interest of the affected DSPs, it is undermined with the catch-all subsection that permits an agency official to include any interests they deem "relevant" [14] in this determination. Moreover, as outlined above, there is no requirement for prior independent review of these notices, nor any independent review of an assessors' determination.

Third, rather than including provisions to promote accountability and transparency, the new law includes extensive secrecy requirements, including authorizing non-disclosure orders that may continue indefinitely, and long after the reasons justifying secrecy have ended.

Taken together, these aspects of the Assistance and Access Act undermine substantive and procedural protections for privacy and civil rights in Australia, and threaten Australia's ability to enter into a bilateral agreement under the CLOUD Act.

**Impact on Industry and Competitiveness**

Earlier reports had forecast that Australia's cybersecurity sector was predicted to triple in size and eclipse revenues of $6 billion AUD by 2026, and would need to fill nearly 18,000 vacancies to achieve this goal.[15] The Assistance and Access Act 2018 undermines the fruition of this estimated need by creating numerous direct and indirect costs to industry. The inability to recruit

[11] Coalition Comment, Open Letter to GCHQ, (May 30, 2019), 3, available at https://newamericadotorg.s3.amazonaws.com/documents/Coalition_Letter_to_GCHQ_on_Ghost_Proposal_-_May_22_2019.pdf.
[12] § 317JAA
[13] § 317P
[14] §§ 317JC(i); 317RA(g).
[15] AustCyber, Australia's Cyber Security Sector Competitiveness Plan, (Nov. 27, 2018), 10, available at https://www.austcyber.com/tools-and-resources/sector-competitiveness-plan-2018.

experts and skilled workers will restrict revenue growth when companies cannot match the growing needs of Australia's cybersecurity sector. Moreover, a decline in users' confidence in Australian device security has already become evident because of this law. The Australian Strategic Policy Institute (ASPI) recently surveyed 512 startups, small to large enterprises, and large bodies in the cybersecurity industry on their views of the economic implications of this law: [16]

- Within the exports sector, 65% of respondents expected the bill to have a negative impact.
- Within the domestic market, 57% of all respondents expected a negative impact upon the industry, and 69% of these respondents found that the impact would last more than two years.
- With device security, 71% of respondents stated that their company's product would be viewed as less secured, consistent with an industry view that Australia's competitiveness would suffer.

While it is difficult to assess with specificity the indirect economic costs of this Act, two things are more certain: (1) the burden of these notices will have anti-competitive effects, and (2) there has already been, and will continue to be, a negative impact on domestic and foreign confidence in Australian telecommunications products and services.

The law makes provision for "reasonable cost" recovery for companies that provide compulsory assistance, but offers no clarity in how providers will seek reimbursement, nor how the reasonable cost determination will be carried out. With DSPs varying in size and nature, so will the notices. As previously argued by the Communications Alliance, this vagueness may result in some providers receiving complex notices that create higher compliance costs and puts them at a disadvantage over others who have either received fewer to no notices or far less intrusive and demanding ones.[17] Moreover, compliance with these notices may result in the creation of inadvertent vulnerabilities and weaknesses, which not only threatens consumers but entire businesses. While the varying nature of these notices is a concern, the overarching problem is the lack of predictability and breadth of these notices, whose harms will negatively impact all recipients regardless of what the actual notice requires.

The PJCIS report found that this new law will negatively impact the perception of this industry by (1) creating a disincentive for foreign investment into the Australian market and/or (2) leading companies to cease ongoing operations in Australia.[18] AustCyber's review has found that companies may become incentivized to design their products in a manner so that providing access is not practicable or technically feasible. This negative perception is not limited to only industry but the education sector as well. Stephen Nagle, executive director of the Holmes

[16] Australian Strategic Policy Institute, Perceptions Survey: Industry views on the economic implications of the Assistance and Access Bill 2018, (Dec. 21, 2018), available at https://www.austcyber.com/resources/perceptions-survey.
[17] Communications Alliance Comment, 20-21, Submission 43
[18] PJCIS report 1.228-9, 82.

Institute, recently noted that prospective students and officials are becoming averse to pursuing higher education and certification in cybersecurity in Australia because students and industry professionals fear that they will not be able to work and conduct research without interference from the government.[19] In particular, Mr. Nagle cautioned how Australia's domestic industry would suffer when the types of research conducted at their institute, such as lightweight encryption for IoT, is no longer sustainable or attractive to students.

These negative perceptions may lead to additional harms by hindering businesses' and consumers' access to new innovations in technology. This in turn could mean that instead of benefiting from new advancements in protecting sensitive personal and financial information, people and businesses will be stuck with outdated security that makes them even more vulnerable to cybercriminals. As Australian encryption technology provider Senetas noted in a recent submission to PJCIS, individuals and organizations will likely become more cautious or reluctant to permit security patches to their systems, something that is critical and fundamental for cybersecurity.[20] This decline of trust in Austrlian cybersecurity will force manufacturers to reevaluate their business plans, and Senetas has stated they will not manufacture in Australia if there was a risk that they would be required to create a backdoor to their products.[21] Aside from the loss of jobs and technical experts this relocation would bring, this distrust will cause Australian cybersecurity R&D and products to suffer within international markets that will see a decrease in the value of Australia's exports market.

**Reporting Obligations and Oversight Measures**

The Assistance and Access Act 2018 also lacks adequate transparency and oversight mechanisms. While we commend the provisions of the law regarding statistical transparency reporting under Sections 317ZF(13) (p. 82) and ZS (p. 106), the strict non-disclosure requirements for companies receiving notices raise serious concerns. The December amendments did authorise a range of further disclosures to enable government officials to confer with one another, and created procedures through which government officials may authorise providers to make certain disclosures regarding technical assistance notices and technical capability notices "in accordance with the conditions specified in the authorisation" (Sec. 317ZF, pp. 73-83). These new provisions, however, do not specify the situations under which providers would be able to obtain such permission, nor do they adequately narrow the broad non-disclosure requirements in the Act.

Rather, Section 317ZF should be further amended to permit designated communications providers to disclose the contents of any technical assistance request, technical assistance notice, or technical capability notice they receive, as well as information about how they responded, unless such disclosure would pose a specific threat to national security, interfere

[19] Denham Sadler, "Encryption bill hits cyber skills," *InnovationAus*, June 12, 2019, https://www.innovationaus.com/2019/06/Encryption-bill-hits-cyber-skills.
[20] Senetas Comment, 3, Submission 85
[21] Extel Comment, 2, Submission 95

with an on-going investigation, or threaten the safety of any person. If a non-disclosure requirement is justified under one of these conditions, the law should limit the duration of the non-disclosure requirement, so that disclosure is permitted after the facts no longer indicate that secrecy is needed.

Finally, the law should be amended to provide for public oversight with additional reporting requirements. For example, it should require the government to conduct a mandatory annual review of the effects and collateral consequences of the issuance of technical assistance notices and technical capability notices, and to make a summary of its conclusions available to the public.

**CONCLUSION**

We continue to have serious concerns regarding the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 due to the threats it poses to cybersecurity, privacy and freedom of expression. As described by U.N. Special Rapporteur on the right to privacy, Joseph Cannataci, "The Assistance and Access Bill is unlikely to be workable in some respects and is an unnecessary infringement of basic liberties in others. The broad drafting provides a high level of discretion on the use of these exceptional powers not to the Parliament but to agencies and the Attorney General. Its aims do not justify a lack of judicial oversight, or independent monitoring, or the extremely troubling lack of transparency."[22] This issue not only deeply affects Australians, but has worldwide implications. We appreciate the government's consideration of our coalition comments, and development of areas of focus for further discussion, but want to reiterate concerns we feel have not been addressed. We hope that these recommendations can provide insight into changes that would be most impactful. While they will not cure every concern that this law raises, these amendments would help to ameliorate some of the most significant problems.

The undersigned organizations and companies appreciate the opportunity to submit these supplemental comments in connection with the Committee's review of amendments to the law.

**Technology Companies and Trade Associations:**

ACT | The App Association
Amazon
Apple
Cloudflare
Computer and Communications Industry Association

[22] Joseph Cannataci, United Nations Special Rapporteur on the right to privacy, Letter regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the Telecommunication and Other Legislation Amendment (Assistance and Access) Act 2018 (Oct. 12, 2018), 16, available at https://www.ohchr.org/Documents/Issues/privacy/O_LAUS_6.2018.pdf.

Dropbox
Facebook
Google
Internet Association
Private Internet Access
Reform Government Surveillance (RGS is a coalition of technology companies)
Startpage.com
Twitter

**Civil Society Organizations**:

Advocacy for Principled Action in Government
Blueprint for Free Speech
Center for Democracy & Technology
Constitutional Alliance
Defending Rights & Dissent
Electronic Frontier Foundation
Engine
Freedom of the Press Foundation
Free Software Foundation
Government Accountability Project
Human Rights Foundation
Human Rights Watch
International Civil Liberties Monitoring Group
Linux Australia
New America's Open Technology Institute
OpenMedia
Open Rights Group
Privacy International
Restore The Fourth
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
TechFreedom
XLab
Xnet