February 21, 2019

RE: International Civil Liberties and Technology Coalition Comments Regarding the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of 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 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 that was enacted in December 2018.[1] We are 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.

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 response to an invitation from the PJCIS.[4] Our November comments noted that although we continued to object to the legislation, we offered suggested changes to the bill that would have mitigated some of the most serious threats that the legislation posed for cybersecurity and individual rights. While we appreciate that the amendments adopted in December took into account some of the suggestions we raised in earlier comments, our most fundamental concerns with the legislation still remain unaddressed.

The Act as enacted threatens cybersecurity and encryption in Australia and around the world. Once Australia uses the broad new powers conferred by the Act to demand that tech companies weaken the security features of their products, this will affect all users of those products,

---

[1] Our comments focus on Schedule 1 (Industry Assistance).

[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)*, September 9, 2018, available at 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*, October 11, 2018, available at 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, November 21, 2018*, available at https://newamericadotorg.s3.amazonaws.com/documents/Australia_supplemental_comments_Nov_21_2018.pdf

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.

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 renew our call for amendments that would mitigate the threats to cybersecurity and human rights that the law poses. These proposals draw from our November comments and explain how the amendments adopted in December fail to redress our key concerns. Thus, the undersigned organizations urge Parliament to consider our recommendations, and make the 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.

In particular, and as outlined further below, Parliament should amend the Act to narrow the technical assistance notice and technical capability notice authorities and further refine the definitions of "systemic vulnerability" and "systemic weakness;" provide for more robust judicial and public oversight of the use of technical assistance notices and technical capability notices, including requiring prior judicial approval and annual reporting; protect the rights of security researchers and software engineers whose work might otherwise be chilled under this new law; and include clear guidance on who is and is not subject to these authorities by limiting the definition of "designated communications providers." Such amendments would constitute a minimum first step to limiting the threats that the law will pose to cybersecurity.

## I. The Act should be narrowed to minimize the threats it poses to cybersecurity and the risks that it would require violations of foreign law

The Assistance and Access Act as enacted added definitions for the terms "systemic vulnerability" and "systemic weakness," and it includes new language in Section 317ZG (pp. 84-85) to clarify that the prohibition against requiring providers to implement a systemic vulnerability or weakness includes a ban on requiring any act that "creates a material risk that otherwise secure information can be accessed by an unauthorised third party." However, these definitions are not clear and specific enough to fully address our concerns about ambiguity or to sufficiently narrow the overly broad 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.

Without additional limiting language, the Act would grant overly broad powers to the Australian government that create risks to device security and cybersecurity more generally. This includes

the risk of what many privacy and security experts colloquially refer to as an encryption backdoor.

For example, the broad powers included in the Act could be read to enable the Australian government to issue notices demanding that providers add the government as a participant in an encrypted chat and suppress the notifications to users that normally accompany such an addition. This idea of adding a "ghost user" has been proposed by officials from the United Kingdom's Intelligence Agency GCHQ,[5] but it would create serious digital security risks. A requirement to add a ghost law enforcement participant would force providers to modify the process of authentication, which normally allows users to have confidence that the other users with whom they are communicating are who they say they are. Like the end-to-end encryption that protects communications while they are in transit, authentication is a critical aspect of digital security and the integrity of sensitive data. Requiring providers to add ghost users would also introduce potential unintentional vulnerabilities, and create new risks of abuse or misuse of systems.

Similarly, there is a risk that the Act could allow the Australian government to compel mobile device makers to create a feature that silently takes periodic screenshots and sends them surreptitiously to the government. The same sort of demand could be used to retrieve photos, videos, documents, or any other piece of data stored on the system.

Additionally, the law must make clear that the government is not authorized to require a designated communications provider to build or implement any specific design of equipment or services; and that the government may not prohibit a designated communications provider from adopting any specific equipment or feature. The law must 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 an individual or entity that uses the provider's product or service.

Finally, the law should include at least three additional limits on the issuance of technical assistance notices and technical capability notices. First, the law should be amended to ensure that a company cannot be compelled to hand over its source code, because any such government demand would irreparably damage users' trust, and could undermine the security of the products or services provided. Specifically, Sec. 317ZH (p. 87) of the law should be amended to include a new paragraph which clarifies that a technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would require a designated communications provider to disclose or provide any source code that it has not already made available publicly or previously disclosed or provided to a government entity.

Second, the law should be amended to clarify that a technical assistance notice and technical capability notice shall not have effect to the extent it requires a designated communications provider to do an act or thing in violation of a foreign country's law. Third, the law should be

[5] Ian Levy and Crispin Robinson, "Principles for a More Informed Exceptional Access Debate," *Lawfare*, November 29, 2018, https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

amended to prevent the government from issuing a technical assistance notice or technical capability notice for the purpose of seeking to preserve its surveillance capabilities. Specifically, the government should not be permitted to issue a notice to prevent a designated communications provider from making subsequent architectural changes to its products or introducing new services if those changes or services might result in a loss of surveillance capability.

## II. The law should be amended to require prior judicial review and a right of appeal

One of the most troubling omissions from the law that still remains is the lack of any requirement for judicial review of technical assistance notices and technical capability notices prior to their issuance. Nor is there a clear and meaningful opportunity for independent or judicial oversight after they have been issued.

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 that would be created by this law, it is critical that the law provide for robust independent oversight of authorising agencies to ensure accountability.

Thus, 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 Federal Court's 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 must 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.

Finally, the law should 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).[6] 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.

## III. The Act should be amended to limit requirements that result in undue secrecy

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

[6] *Telecommunications and Other Legislation Amendment (Assistance And Access) Act 2018 Explanatory Memorandum*, House Of Representatives, Commonwealth Of Australia, available at https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf;fileType=application%2Fpdf

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 threat to national security, interfere with an 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. The law’s contemplation of criminal penalties for employees of designated communications providers is unnecessary and only serves to chill employees’ ability to seek counsel from their superiors or discuss technical aspects of a given notice with responsible parties within the company. The law should only hold a company, not any specific employee or person, liable for any violation of disclosure prohibitions. Additionally, the law should be amended to permit designated communications providers that receive a notice but are not subject to a non-disclosure requirement to notify the target of that notice.

The law should also be amended to ensure that it does not chill the activities of security researchers or software engineers. Specifically, language should be added to the law that explicitly protects from liability any person or entity who independently discovers a change that was made to a technology pursuant to a government notice, and then discloses or provides technical information about the change. Similarly, the law should also be amended to ensure that no one is forbidden from attempting to discover such changes in the first instance, or from creating infrastructure that might facilitate others in discovering them.

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.

## IV. Definition of designated communications providers should be narrowly tailored

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 fora, 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 needs to 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.

## V. 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. We appreciate the government's willingness to consider further amendments to the law, and we hope that these recommendations can provide guidance as to some 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 threats.

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.

**Civil Society Organizations**:

Access Now
Blueprint for Free Speech
Center for Democracy & Technology
Constitutional Alliance
CryptoAUSTRALIA
Defending Rights & Dissent
Electronic Frontier Foundation
Electronic Privacy Information Center
Engine
Enjambre Digital
Freedom of the Press Foundation

Government Accountability Project
Human Rights Watch
International Civil Liberties Monitoring Group
Linux Australia Inc.
New America's Open Technology Institute
Open Rights Group
Privacy International
Restore The Fourth, Inc.
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
TechFreedom
X-Lab
World Privacy Forum

**Technology Companies and Trade Associations**:

ACT | The App Association
Amazon
Apple
Cloudflare
Computer & Communications Industry Association
Facebook
Google
Internet Association
Microsoft
Reform Government Surveillance (RGS is a coalition of technology companies)
Startpage.com
Tenable
Twitter