November 21, 2018

RE: 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

To whom it may concern:

In response to the invitation of the Parliamentary Joint Committee on Intelligence and Security (PJCIS), by email of October 28, 2018, to submit further comments on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 being considered by the Committee, the undersigned organizations and companies jointly submit these supplemental comments.[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.

The undersigned organizations and companies are part of a coalition that previously raised significant concerns with the bill as introduced in comments submitted on October 11, 2018.[2] As we noted, while we appreciate that the bill before the PJCIS includes several important improvements upon the initial Exposure Draft, the vast majority of the concerns we identified in our original comments concerning that draft[3] were not addressed. For example, the section of the bill creating the new authorities to issue technical assistance requests (TARs), which seek voluntary assistance from communications providers; and technical assistance notices (TANs) and technical capability notices (TCNs), both of which require providers to do one or more specified acts or things, would confer overly broad authorities that would undermine cybersecurity and human rights, including the right to privacy. Additionally, the bill fails to provide adequate oversight over these new authorities; it creates undue secrecy for the use of these new tools; and it includes an overly broad definition of "designated communications providers."

In light of these outstanding concerns, we continue to object to the adoption of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill. However, if the Parliament pursues passage of this bill, its sponsors should, at the very least, adopt

[1] Our comments focus on Schedule 1 (Industry Assistance).
[2] Coalition comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on 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.
[3] Coalition comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the Exposure Draft of the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 (Sept. 9, 2018), https://newamericadotorg.s3.amazonaws.com/documents/Coalition_comments_on_Australia_bill.pdf.

certain critical amendments. These changes would ameliorate, though not cure, some of the most significant concerns the bill would raise.

In particular, and as outlined further below, Parliament should adopt amendments that will narrow the Technical Capability Notice and Technical Assistance Notice authorities to help ensure they do not threaten cybersecurity; provide for more robust judicial and public oversight of the use of these authorities, 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 bill poses to cybersecurity.

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

As noted in this coalition's previous comments, the explicit statement in the bill that providers "must not be required to implement or build a systemic weakness or systemic vulnerability" and that the government must not prevent communications providers "from rectifying a systemic weakness, or a systemic vulnerability" is essential to ensuring the bill does not harm cybersecurity (Sec. 317ZG, p.52). However, without additional limiting language, the bill would nonetheless 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.

In order to reduce these risks, the bill should incorporate a clear definition for "systemic vulnerability or weakness." The current draft of the bill provides no definition at all, which leaves this critical term open to interpretations that would permit government demands that appear to apply narrowly, but could have far broader effects. To prevent such an interpretation from being applied to these authorities, the bill should be amended to define "systemic vulnerability or weakness" to 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.

Additionally, the bill should 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 bill 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 an individual or entity that uses the provider's product or service.

Finally, the bill should include at least three additional limits on the issuance of technical assistance notices and technical capability notices. First, the bill 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 of the bill 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, Sec. 317ZX 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 bill should be 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 bill should be amended to require prior judicial review and a right of appeal

One of the most troubling omissions from this bill 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. As we noted in previous comments, given the breadth and power of the new authorities that would be created by this bill, it is critical that the law provide for robust oversight of authorising agencies to ensure accountability.

At a minimum, that bill 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 and Section 317ZH; 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.

Additionally, Sec. 317W, which would govern consultations about proposals to issue technical capability notices, should be amended to provide for review by the Federal Court. If the report of the assessment prepared pursuant to the consultation process, as required under paragraph (7) of this section, raises significant concerns regarding the proposed technical capability notice, the Attorney-General must be required to seek review by the Federal Court before it can give such technical capability notice. The Federal Court would then be required to review whether the government's interest in giving the technical capability notice is so great that it significantly outweighs the concerns raised in the report of the assessment.

Finally, the bill 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 (p. 51) of the bill 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 bill 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, new Section 317ZFA 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 states that these notices are not subject to a merits review (pp. 15, 29, 60). Moreover, given the bill'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 bill should be amended to limit requirements that result in undue secrecy

While we commend the provisions of the bill regarding statistical transparency reporting under Sections 317ZF(13) and ZS, the strict non-disclosure requirements for companies receiving notices raise serious concerns. To address these concerns, Section 317ZF of the bill should be 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 bill 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 bill'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 bill should only hold a company liable for any violation of disclosure prohibitions. Additionally, the bill 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.

Additionally, the bill should be amended to ensure that it does not chill the activities of security researchers or software engineers. Specifically, language should be added to the bill 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 bill 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 bill 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 bill for "designated communications providers" is overly broad. As our coalition noted in a previous submission, 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 bill, "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 draft bill, this includes anyone who "provides an electronic service that has one or more end-users in Australia." (Sec. 317C). Under the Explanatory Memorandum, "electronic service” is also broadly defined, and “may include websites and chat for a, 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 bill makes clear that the orders can be served outside Australia (Sec. 317ZL).

To address these concerns, Section 317C of the bill should be 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 object to the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 due to the threats it poses to cybersecurity, privacy and freedom of expression. However, if the Parliament pursues passage, its sponsors should, at the very least, adopt the amendments described above. While they will not cure every concern that this bill raises, these amendments would ameliorate some of the most significant of those concerns.

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

Civil Society Organizations:

Australian Information Security Association
Blueprint for Free Speech
Center for Democracy & Technology
CryptoAUSTRALIA
Defending Rights & Dissent
Electronic Privacy Information Center
Engine
Enjambre Digital
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.
R Street Institute
X-Lab

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
Twitter