October 11, 2018

RE: 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:

The undersigned organizations and companies jointly submit these comments regarding the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 being considered by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). 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. Although we commend several provisions of the draft bill, we submit these comments to outline our shared concerns that the proposed legislation poses serious threats to cybersecurity, privacy, and freedom of expression. Many of our organizations and companies previously submitted similar comments on September 9, 2018 regarding the Exposure Draft of the Assistance and Access Bill 2018, and the vast majority of the concerns we identified have not been addressed by the updated version of the bill.

We welcome the statement in Section 317ZG of the draft bill that communications providers "must not be required to implement or build a systemic weakness or systemic vulnerability" and that the government may not prevent providers "from rectifying a systemic weakness, or a systemic vulnerability." However, other sections of the bill undermine the safeguards provided by this language, thereby threatening encryption and cybersecurity more generally, as well as fundamental human rights, including the right to privacy.

As many of the undersigned organizations and companies previously noted in a May 2015 letter and subsequent letters to Ministers of the Five Eyes security community and the Australian government, strong encryption is the cornerstone of the modern information economy's security.[1] 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.

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

[1] *See* Coalition letter to President Barack Obama (May 19, 2015), https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf; Coalition letter to Ministers responsible for Five Eyes Security Community (June 30, 2017), https://www.accessnow.org/cms/assets/uploads/2017/07/Five-eyes-open-letter.pdf; *and* Coalition letter to Australian government officials (July 17, 2018), https://www.accessnow.org/cms/assets/uploads/2018/07/Australia-Encryption-Coalition-Letter.pdf.

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."[2] 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 as troubling Australia's intention to model this approach.[3] 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.

Among other provisions, the draft bill authorises the Australian government to use three new tools to seek or compel assistance from technology companies in accessing electronic communications information. These tools are 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. The section of the bill creating these new authorities includes some commendable safeguards, but it also raises many serious concerns. Specifically, the new technical assistance notices and technical capability notices are overly broad authorities that would undermine cybersecurity and human rights, including the right to privacy; the bill fails to provide adequate oversight over these new authorities; the bill creates undue secrecy for the use of these new tools; and the bill includes an overly broad definition of "designated communications providers." While the revised version of the bill does make some positive changes – such as eliminating "protecting the public revenue" as a rationale for data requests and demands – the updated version still presents these four key concerns that we have identified.

## I. The bill creates overly broad powers that threaten cybersecurity

As noted above, we commend the explicit statement 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." (Sec. 317ZG, p. 52). However, the bill nonetheless grants 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.

[2] 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, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement.
[3] 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), paragraph 14, https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf.

The broad language authorising technical assistance notices and technical capability notices undermines the prohibition of requiring a "system weakness." The list of "acts or things" that providers can be compelled to do/provide is very broad and includes such items as "(a) removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider...(c) installing, maintaining, testing or using software or equipment…(f) assisting with the testing, modification, development, or maintenance of a technology or capability, or…(h) modifying, or facilitating the modification of, any of the characteristics of a service provided by the designated communications provider" (Sec. 317E (1), pp. 15-16). Installing unknown and untested software risks introducing new vulnerabilities into a system. Moreover, users may perceive the surreptitious introduction of any new code into a complex technology environment as the Government requiring the installation of malware.

We also caution against requiring communications providers to take any action that would threaten the integrity and trustworthiness of routine update procedures. A working group of the United States' National Security Council previously considered several technical "proofs of concept," including one for "provider enabled remote access to encrypted devices through current update procedures." The National Security Council strongly warned against this approach, stating that:

> "[I]ts use could call into question the trustworthiness of established software update channels. Individual users, concerned about remote access to their devices, could choose to turn off software updates, rendering their devices significantly less secure as time passed and vulnerabilities were discovered b[ut] not patched."[4]

The language in the draft bill also appears to permit the type of demand that the U.S. Federal Bureau of Investigation (FBI) made in 2016 when it sought a court order to compel Apple to help unlock an iPhone belonging to a suspect in the shooting in San Bernardino, CA, the previous year. In that case, the FBI wanted the court to require Apple to develop a new operating system that would circumvent critical passcode authentication security features.

Apple challenged the legality and constitutionality of the court order, and dozens of other technology companies, security experts, and privacy advocates wrote to the court to voice their opposition as well. The FBI argued that this request would only apply to a single device in that particular case. While the FBI was not technically seeking a "systemic" solution (i.e. one that would automatically apply to every phone), it was still seeking a means of access that would have systemic effects. As Apple noted when it explained why it was challenging the FBI's demand,

> "Once created, the technique could be used over and over again, on any number of devices. In the physical world, it would be the equivalent of a master key,

[4] Obama Administration Draft Paper on Technical Options, p. 6, http://apps.washingtonpost.com/g/documents/world/read-the-obama-administrations-draft-paper-on-technical-options-for-the-encryption-debate/1753/.

> capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes."[5]

Moreover, the real challenge in developing systems for exceptional access to encrypted data -- whether through software updates, installing a new operating system, or employing some other solution meant to be employed on a case-by-case basis -- is ensuring that the system implementing the exceptional access method is secure. Susan Landau, the Bridge Professor in the Fletcher School of Law and Diplomacy and the School of Engineering, Department of Computer Science, Tufts University, recently explained this problem in a post on the national security themed blog, *Lawfare*:

> "Building [an exceptional-access] system would be extraordinarily hard and would require a large team of engineers. An exceptional-access system would have to operate in real time, authenticate multiple law-enforcement agencies (including police and sheriff departments, of which there are over 15,000 in the U.S.), ensure the accuracy of the authentication system and its ability to withstand attacks, and handle frequent updates to hardware, the operating system, phones, and more. The exceptional-access system would have to be flexible enough to handle the varied architectures of different types of phones, security systems and update processes. (The latter would be extremely challenging for phones using the Android operating system, which are supplied by multiple different vendors. These providers often customize the open-source Android release to some extent—and may make changes on varying schedules. Thus the diversity of Android devices is likely to make subverting them through a software update significantly harder than it would otherwise be.)."[6]

The draft bill's list of "acts or things" does not take into account how difficult those mechanisms for access to data would be for technology companies to implement. It also fails to address how dangerous they would be to users' security, given the significant likelihood of a flaw in the process implementing the exceptional access mechanism. Instead, the bill requires only that the government official issuing a technical assistance notice (Section 317P, p. 28) or technical capability notice (Section 317V, p. 36) be satisfied that the requirements are reasonable and proportionate, and that compliance with the notices is practicable and feasible. For technical capability notices, the revised version of the bill does add a new Section 317ZAA (p. 41) which sets forth "matters" that the Attorney-General must consider in assessing whether a notice is reasonable and proportionate, but this remains a subjective standard based on the government's views and not the views of the company or security experts. In the U.S. context, we have already seen that what the government views as reasonable, as illustrated by the FBI's

[5] A Message to Our Customers, Apple (Feb. 16, 2016), https://www.apple.com/customer-letter/.
[6] Building on Sand Isn't Stable: Correcting a Misunderstanding of the National Academies Report on Encryption, *Lawfare* (April 25, 2018), https://www.lawfareblog.com/building-sand-isnt-stable-correcting-misunderstanding-national-academies-report-encryption.

litigation against Apple in 2016, can be widely considered to be unreasonable and impracticable.

The revised bill helpfully adds a process for an assessment of whether a proposed technical capability notice would violate Section 317ZG's prohibition on demands that cause a systemic weakness (Section 317W, pp. 37-38), but this new provision is not sufficient to mitigate the potential harms from technical capability notices. The new portion of Section 317W states that a provider receiving a "consultation notice" for a proposed technical capability notice, may, jointly with the Attorney-General, appoint a person to assess the terms of the notice, and prepare a report examining whether it would violate the prohibition on notices that would cause a systemic weakness. The new provision also states that the Attorney-General must subsequently consider any such report before issuing a technical capability notice. However, the new provision does not narrow the scope of permissible technical capability notices, and, as outlined below, it still leaves the decision to the Attorney-General without any prior independent review.

While the government would generally be required to offer the subject of a technical capability notice an opportunity to submit comments on the proposed notice before it goes into effect, any comments must be submitted and considered by the government in only four weeks. This time-frame is unduly short, and the requirement for a four-week consultation process does not even apply if the government determines that issuing the technical capability notice is a matter of urgency, or that engaging in the consultation is impracticable (Section 317W, p. 37).

## II. The bill fails to provide adequate authorisation, right of appeal, and oversight

The draft bill fails to provide adequate oversight for the new technical assistance notice and technical capability notice authorities, either before or after issuance of these government demands.

First, we are concerned that no prior independent review is required before the government may issue a technical assistance notice or technical capability notice. The bill's provisions creating these authorities have been modeled on the United Kingdom's new Investigatory Powers Act (IPA). We also have concerns about the overbreadth and oversight of authorities under the UK law, but Section 254 of the UK's IPA does require that Judicial Commissioners must review proposed technical capability notices before such a notice may be issued. While questions remain as to the adequacy and independence of this review, there is no provision requiring any type of prior, let alone independent, review under Australia's draft bill.

Second, the bill does not create a clear process or standard for challenging technical assistance notices or technical capability notices. The Explanatory Memorandum released with the new version of the bill states that "Australian courts will retain jurisdiction for judicial review of a decision" to issue a notice, and that this "will ensure that an affected person, or a provider o[n] behalf of an affected person, has an avenue to challenge unlawful decision making" (p. 14).

New Section 317ZFA (p. 51) of the revised 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 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 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.

Finally, the bill fails to provide for any review or independent oversight of technical assistance notices or technical capability notices after they have been issued. 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.

## III. Despite permitting statistical transparency, the bill requires undue secrecy

We commend the provisions of the bill regarding statistical transparency reporting, but the strict non-disclosure restrictions for companies receiving notices raise serious concerns.

Importantly, Section 317ZF(13) (pp. 50-51) permits communications providers to disclose the total number of each type of government request or notice -- technical assistance requests, technical assistance notices, and technical capability notices -- that they receive during a period of six months. Permitting companies to include these statistics in their regular periodic transparency reporting is critical to promoting public trust and accountability. Further, Section 317ZS (p. 67) of the draft bill requires that the government issue annual reports that disclose the total number of technical assistance requests, the total number of technical assistance notices, and the total number of technical capability notices that the government issued during the prior year. This transparency provision is also commendable.

However, these provisions are insufficient to provide meaningful accountability, because the draft bill also contains strict non-disclosure requirements that impose undue secrecy. These rules make it a criminal offense to disclose any information about particular requests or notices. Under Section 317ZF (pp. 45-47) of the bill, individuals who disclose information regarding a technical assistance request, technical assistance notice, or technical capability notice, may be subject to imprisonment for five years. The exceptions permitting disclosure are extremely narrow, and generally only permit disclosures for the purpose of carrying out the government request or demand. Although company personnel are permitted under Section 317ZF(3) (p. 48) to make disclosures for the purpose of seeking legal advice, they are otherwise prohibited from

revealing any information about any technical assistance request, technical assistance notice or technical capability notice.

These non-disclosure rules apply to every type of technical assistance request, technical assistance notice, or technical capability notice. Non-disclosure requirements are not limited to certain types of cases, such as where disclosure would provide a threat to national security, interfere with an investigation, or threaten the safety of any person. Nor is there any time limit provided for the non-disclosure requirements. The bill fails to include a provision permitting disclosure after the facts no longer indicate that secrecy is needed. These mandates for such complete secrecy are unnecessary, and strict limits to non-disclosure rules are needed to promote government accountability.

## IV. The definition for “designated communications providers” is overly broad.

The definition in the bill for "designated communications providers" is overly broad. It could affect hundreds of thousands, if not millions, of individuals in Australia and around the world. As the Explanatory Memorandum describes, "designated communications provider" under the new law 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, p. 12). 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 bill makes clear that the orders can be served outside Australia (Sec. 317ZL, pp. 58-60).

As a consequence, Australian law enforcement and intelligence services will be able to serve technical assistance and capability notices (with corresponding confidentiality requirements) on a large number of companies and individuals involved in almost every element of the communications industry. Under this reading, the maintainers of journalistic news sites or of religious groups’ mailing lists, and system administrators of the communications networks of political parties, could be served. A significant number of core Internet services -- including key software development, the management of software updates, and the provision of certification services that assert the authenticity and identity of websites and communication endpoints -- would also be affected.

The potential impact is even more concerning because many of the individuals who would qualify as "service providers" are volunteers. For instance, many Australian companies and citizens use the operating system GNU/Linux, which has thousands of individual contributors. One of the popular methods for installing and maintaining this operating system is provided by Debian, a community whose legal entity is a United States non-profit, Software in the Public Interest, but whose infrastructure and services are provided by volunteers. Many GNU/Linux contributors and Debian volunteers are based in Australia, and could be defined as "service providers" under the current draft of the bill. Under the draft bill, these volunteers could be

compelled to modify or substitute any part of the software or service they provide, and conceal this from their users.

The impact of secret orders served on individuals acting in their own personal capacities is very different from a set of law enforcement agreements with major telecommunications companies. A telecommunications company may be able to defend itself through a legal challenge whereas individuals often could not. The disproportionate power of the state in forcing a single person to change their behavior without being permitted to discuss what they are being compelled to do requires a much higher standard of oversight and transparency.

## V. Conclusion

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

**Civil Society Organizations**:

Access Now
Advocacy for Principled Action in Government
Blueprint for Free Speech
Center for Democracy and Technology
Constitutional Alliance
CryptoAUSTRALIA
Defending Rights & Dissent
Electronic Frontier Foundation
Electronic Frontiers Australia
Electronic Privacy Information Center
Engine
Enjambre Digital
Freedom of the Press Foundation
Free Software Foundation
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
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
World Privacy Forum
X-Lab

**Technology Companies and Trade Associations**:

ACT | The App Association
Amazon
Apple

Cloudflare
Computer & Communications Industry Association
Facebook
Google
i2Coalition
Internet Association
Microsoft
Reform Government Surveillance (RGS is a coalition of technology companies)
Startpage.com
Twitter

Coalition comments submitted by:
Sharon Bradford Franklin
Director of Surveillance & Cybersecurity Policy
New America's Open Technology Institute
740 15th Street NW, Suite 900
Washington, DC 20005