accessnow

Parliamentary Joint Committee on Intelligence and Security (PJCIS)
PO Box 6021, Parliament House
Canberra ACT 2600
TOLAbill@aph.gov.au
Attn: Secretariat

Re: Telecommunication & Other Legislation Amendment (Assistance & Access) Bill 2018

November 2018

To Whom It May Concern,

Thank you for the additional opportunity to provide feedback to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (hereafter, "Assistance and Access Bill" or "the Bill").[1]

In our previous submission we identified several areas where the legislation could be improved. In particular, we encouraged you to separate Schedule 1 and Schedule II and to consider these sections separately. Specifically we recommend to the Committee:

- *Schedule 1 and Schedule 2 should be intentionally divorced from one another and considered separately and with intention to provide full and complete understanding of how each will operate in the current legislative environment;*
- *Given its hithertofore absence from public debate, consideration of Schedule 2 should be postponed for further debate and additional opportunity for public comment pending the availability of information to further contribute to the understanding referenced above[.]*

The authorities to issue Technical Assistance Requests (TARs), Technical Assistance Notices (TANs), and Technical Capability Notices (TCNs) are far-reaching and will have global impact. Further Schedule 2 would facilitate government hacking, "one of the most invasive government surveillance activities in the modern world. All government hacking substantially interferes with human rights, including the rights to privacy and freedom of expression."[2]

These extraordinary powers to be assumed by the government should be supported by a comprehensive factual record explaining what problem the authority is seeking to solve and the connection between the solution and the problem. Evidence-based decision making is a

[1] https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018.
[2] See https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

fundamental component of good governance and a critical step to ensure that democratic institutions remain free from undue political influence.[3]

Evidence is particularly important in regard to proposed legislation that will have as broad an impact as the Assistance and Access Bill. However, the government has supported its call to implement the Bill using only vague references and unsupported statistics on how encryption is used by criminals. These statements are insufficient to justify the incursions the Bill would authorise. Accordingly, any further debate on this legislation should be immediately suspended unless and until the government can provide necessary details about its requirements, including:

- What types of encryption being encountered as a barrier to investigation;
- How and why alternative investigative methods have failed;
- The specific ways that Assistance and Access would remedy these failures;
- What reporting will be provided to Parliament to maintain continued oversight of the challenges faced by law enforcement.[4]

Until these questions are answered on the public record, we continue with our strong recommendation that the entire Assistance and Access Bill be tabled in order to pursue an approach that will provide law enforcement entities with meaningful tools and education on access to data necessary for investigations without implicating secure tools or services that internet users across all sectors rely upon.

The importance of a strong factual record was recognized by the European Union in 2016. Prior to taking action similar to that being proposed in Australia, the Slovak Presidency to the Council of the European Union shared a questionnaire with members of the Justice and Home Affairs Council. The questionnaire asked members to provide details about any national legislation they have on encryption and to what extent law enforcement activities are impacted by encryption.[5] The responses demonstrated that while law enforcement was facing issues in regard to investigations involving digital evidence, the number of cases which were truly impeded by encryption were few across all EU member states. In order to better document the process, this has since led to several coordinated efforts to provide additional resources for those issues.[6] Based on the state responses, the Commission decided not to pursue a path that would impact encryption and instead decided to explore other areas.[7] Such a process would greatly benefit Australia.

## I. There is an insufficient factual record to justify the implementation of the Assistance and Access Bill, particularly in light of its potential ramifications

[3] *See, e.g.*, https://www.cep.gov/content/dam/cep/report/cep-final-report.pdf.
[4] https://www.homeaffairs.gov.au/consultations/Documents/explanatory-document.pdf.
[5] https://www.accessnow.org/eu-ministers-targeting-encryption-need-know/.
[6] https://www.accessnow.org/mixed-messages-crypto-closed-door-conversations-eu/.
[7] https://www.accessnow.org/european-commission-thinking-government-hacking/.

As previously stated, the explanatory document from the exposure draft of the Bill explained that "95 per cent of the Australian Security Intelligence Organisation's (ASIO) most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications," a claim echoed by ASIO Director-General Duncan Lewis in an opinion-editorial published by *The Australian*.[8] This statistic is offered without evidence or citation. There is no indication of what type of encryption that the statistic refers to, what type of information it prevents access to, or what methodology was used to arrive at that number.

Additionally, the public has not been provided with adequate information about the presumptive targets who are using encryption. The Department of Home Affairs included a narrative example intended to support the adoption of the Bill. Instead, a careful reading of this example provides evidence instead of why the Bill is not necessary. Here is the relevant portion of the example:

> *The suspect was arrested and his mobile phone was seized but despite legislative requirements he refused to provide his passcode. Due to an inability to access his phone as well as the fact that he used encrypted communication methods such as Snapchat and Facebook Messenger, Victoria Police was unable to access evidence which would have enabled them to secure a successful prosecution and identify further victims and offences.*

First, this example does not take into account the availability of metadata from providers (which is not encrypted) in order to determine connections between the suspect and other potential victims. Additionally, it ignores the availability of content evidence through the devices of the victims themselves, as well as other potential victims identified through the use of metadata. Finally, it pre-supposes that Snapchat and Facebook Messenger are "encrypted communication methods." The encryption used by either service by default does not hide content from the providers, and therefore would not prevent law enforcement from receiving that content subject to valid process, which should satisfy human rights standards.[9] Finally, this example also ignores certain realities, including how criminals and terrorists, who are ever-increasingly savvy with technology, will likely respond to the Assistance and Access Bill, or anything like it, by switching to services outside of Australia's jurisdiction.

## II. Alternative options are available to assist law enforcement in obtaining information necessary for investigations

In addition to failing to provide an adequate factual record, the Assistance and Access bill does not address issues that could markedly improve law enforcement's abilities in the digital era. There are many questions at the intersection of crime and technology. As the Joint Committee on Law Enforcement has seen in their examination of law enforcement in the digital era, these

[8] https://www.homeaffairs.gov.au/consultations/Documents/explanatory-document.pdf;
[9] *See*, *e.g.*, https://www.bbc.com/news/newsbeat-43485511.

problems can include difficulties accessing data, lack of awareness regarding what data exists, difficulty accessing data oversees, and slow processes for interacting with technology companies that hold the data.

More information could help identify and fill these policy gaps and inform the public debate regarding lawful access to data. For example, corporate representatives could teach officers the most expedient ways to lawfully request information they already have authority to receive, including metadata as well as communications content when pursuant to the proper legal process. This is a process many companies have already initiated.[10] Other options to pursue include education for law enforcement about 1) what data actually exists and where to access it; 2) how to properly submit data requests to companies at scale; 3) paths to obtain data from companies overseas, and particularly the delays involved in the Mutual Legal Assistance (MLA) process, and 4) how to use certain types of data in legal proceedings.

These are issues that the Department of Home Affairs could address without undermining encryption and cybersecurity. And in fact, the emphasis at Home Affairs on encryption has meant that there has been little progress on these other issues. Just recently, the United States passed new legislation that enables the U.S. Department of Justice to negotiate bilateral treaties to allow foreign government officials to apply their domestic laws directly to access data held by a company in the United States. Under current law, Australia is not taking advantage of its relationship with the United States. While the new law itself fails to provide adequate protections, and any arrangement under this legal authority should include additional human rights protections, an agreement would grant Australian law enforcement significantly greater access to digital data.

## Conclusion

Thank you for consideration on this important issue. We appreciate your time and attention. If you have any questions about this submission or any other issues raised by the Assistance and Access Bill you can contact the undersigned.

Sincerely,

Amie Stepanovich
Global Policy Counsel
Access Now

Nathan White
Senior Legislative Manager
Access Now

[10] *See, e.g.*, https://www.washingtontimes.com/news/2018/sep/5/apple-team-will-train-law-enforcement-digital-fore/.