From: Andrew Donnellan
To: Assistance Bill Consultation
Subject: Submission on Assistance and Access Bill 2018
Date: Monday, 10 September 2018 3:30:48 PM

Dear sir/madam

I thank the Department of Home Affairs for the opportunity to make a submission regarding the exposure draft of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 ("the Bill").

As an IT industry professional, I have deep concerns about the Bill as it currently stands. While I understand the Government's desire to enable our law enforcement and national security agencies to continue protecting Australia in a changing technological environment, I believe this Bill poses problems for the protection of Australians' personal privacy and security.

I expect that the Department has received many submissions from members of the technology and information security communities that articulate the major reasons why this Bill is problematic. I will not repeat those objections here, other than to say that I broadly agree with the position that this Bill goes too far. I will confine this submission to a small number of specific issues that stand out to me as areas where the Bill could be substantially improved without major changes.

1) Independent oversight of TARs, TANs and TCNs

In the proposed Bill, the issuance of TARs, TANs and TCNs does not require approval from outside the agency, apart from TCNs requiring the approval of the Attorney-General.

In my opinion, for the more serious types of notices, especially TCNs, it would be appropriate for the issuance of such notices to require the ultimate approval of an independent body. Such an independent body could be a court or judicial officer, however given the highly technical nature of these requests the establishment of an independent commissioner could be more appropriate. Ministerial oversight and after-the-fact disclosure and review alone is insufficient to ensure public confidence that the TAN and TCN regime is not being abused.

2) TAN/TCN reporting requirements

The reporting requirements in the Bill for TANs and TCNs only extend to reporting the numbers of TANs and TCNs issues.

In my view, merely knowing the numbers does not provide sufficient information for the community to understand the impact that these notices are having on privacy and security. While it is understandable that the Government would not wish to disclose sources and methods in too much detail, it is vital that the Bill's reporting requirements mandate disclosure of some level of detail of the types of capabilities that the Government has required, in order to inform public debate and technical research.

3) Mandatory review and sunset clause

In recent years, we have seen a rapidly changing technological, geopolitical and security environment, including the ever-increasing penetration of technologies including mobile telecommunications, artificial intelligence and social media into every area of life, and the

public disclosure of signals intelligence and offensive cyber activities led by both democratic and authoritarian governments. Amidst this, governments, the technology industry, civil society and the general public have been renegotiating the social licence under which the technology industry operates, as seen through the public discourse surrounding the role of social media platforms, the adoption of the EU General Data Protection Regulation, and the debate surrounding Five Eyes SIGINT activities.

In light of this, it is appropriate for the powers granted by this Bill to have a mandatory review and sunset clause in at most 5 years' time, and preferably a shorter period such as 3 years. Whilst sunset clauses in national security legislation have traditionally been of limited utility in protecting civil liberties, it is important given the constantly shifting public debate to ensure that Parliament reviews the situation in a timely fashion.

Such a review should involve the Independent National Security Legislation Monitor, and should also involve representatives from civil society, academia and industry to ensure appropriate representation of the public interest and access to technical knowledge required to properly assess the impact of this Bill on cyber security and civil liberties.

Conclusion

It is important that in light of the current trend towards better recognition of user privacy interests, the Australian Government must work towards policy which achieves its legitimate goals without compromising Australians' right to privacy. I continue to have my doubts that the objectives of this Bill can be achieved without significant privacy concerns, however if this Bill is going to be enacted, it must, at the very least, contain stronger safeguards and stronger accountability mechanisms that will inform the public debate on whether these measures continue to be appropriate.

Yours sincerely

Andrew Donnellan BA BSc(Hons) (ANU)