Australian Computer Society Inc. (ACT)
ARBN 160 325 931

National Secretariat
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

10 September 2018
The Director General,
Department of Home Affairs

ACS submission on the Assistance and Access Bill 2018

Dear Director General,

Thank you for the opportunity to contribute to this discussion.

The Australian Computer Society (ACS) is the professional association for Australia's information and communications technology (ICT) sector. We are passionate about the ICT profession being recognised as a driver of innovation and business – able to deliver real, tangible outcomes.

Our vision is for Australia to be a world leader in technology talent that fosters innovation and creates new forms of value. We have over 42,000 members and seek to influence positive change within industry and in the area of public policy via publications that leverage the knowledge capital of ACS members.

We write now to voice our concern about the proposed Telecommunications & Other Legislation Amendment (Assistance & Access) Bill 2018. Many of our members have raised issues with the bill, including members of our expert Cyber Security Technical Advisory Board, which is comprised of some of the most experienced and well known cyber security professionals in Australia.

While our members share a strong respect for the need for properly authorised law enforcement and security agencies to have access to communications services, in our view the legislation appears to have insufficient oversight and protections.

Key issues

We believe that there are a number of key issues that need to be resolved before the Bill goes into law:

1. The breadth of access is greatly concerning as it applies to devices and systems beyond those ordinarily used in telecommunications services (for example internet connected appliances). Under the Bill, organisations with no cybersecurity or regulatory understanding will have obligations to comply that they cannot properly fulfil due to a lack of expertise. Such an organisation, under this legislation, will require the expertise to properly implement systems as required by law enforcement – skills they may not normally have and will be unable to ensure remain risk or

trouble free. This imposes significant privacy and security risks to Australian homes and organisations.

2. From the perspective of business planning, it is very difficult to plan for the requisite resourcing this legislation may require. This level of obligation would unfairly impact smaller providers.

3. The breadth of the proposed legislation extends beyond national security to the protection of public revenue (i.e. beyond simple taxation assurance) and even to the protection of Australia's economic interest which has undertones of spying and should not be covered in the scope of these interception measures.

4. This legislation acts as a powerful disincentive for foreign companies to set up in Australia as it exposes them to onerous compliance obligations, and does not provide sufficient protections for customer data.

5. It further acts as a disincentive to Australian organisations providing services overseas. We believe this legislation will disadvantage Australian cyber and communications companies on the global stage. The government has limited powers to force overseas companies to comply – it will likely never be able to force compliance from Signal creators Open Whisper Systems, for example. However, Australian companies will be completely subject to it. This in turn can erode the trust in these companies, and even potentially result in a diaspora of Australian cyber security and communications companies. The Australian Government has recently banned 5G products from companies likely to "be subject to extrajudicial directions from a foreign government." For other countries, the Australian government will be foreign to them, therefore should they have similar provisions in place Australian companies may well be excluded from providing equipment or services due to this legislation.

6. It is likely not possible to build in functions to get around encryption without building in systemic weakness or vulnerability into a given product or service. The current approach of the legislation exposes internet and private telecommunications users – business and personal alike – to the potential for very real risks to their privacy and reliability of these services.

7. Whilst the Bill Explanatory Document goes to some length to describe the safeguards that agencies choose to put place, these are not replicated in the bill itself, or significantly watered down, so if passed as it is, the law will not require that agencies do what the explanatory document says they will.

8. There is a concern to the broad nature of persons who could be the subject of an assistance notice and the temptation for agencies to utilise assistance notices without first trying and exhausting other means.

9. There is no requirement for those obligated to provide assistance to maintain confidentiality or have security clearance.

10. There are concerns regarding the ability for agencies to alter a targeted computer and lack of safeguards against agencies altering (including removing) data needed to prove innocence.

Recommendations

We propose the following needs to be undertaken before a Bill is passed into law:

1. Further analysis needs to be undertaken to understand the burden this Bill will create for local Australian businesses and their ability to be able to compete effectively in the international market.

2. Further studies are needed to better understand the potential for introducing additional privacy and disruption of service risks to Australian individuals and businesses.

3. Safeguards outlined within the Bill Explanatory Document need to be consistent with the Bill itself.

4. Decision-making criteria should be amended to include the need for agencies to have exhausted (i) their own means and (ii) commercially procured means. Also, that arriving at the decision to use an assistance request, the agency document the means that they have already tried and/or tried to procure. At present, there is no requirement for the Agency to have first tried to access the communications or data themselves.

5. That the Government set up an expert committee to review the use of the above, perhaps annually. This is an area where the ACS may be able to assist, as a number of members already have the NV2 and above security clearances that would be needed for such purposes.

6. That the Government create a mechanism for the payment of reasonable fees to subjects that are compelled to provide support to the Government.

7. That agencies are required to disclose when evidence has been altered in compliance with a warrant and set out specific items have been altered. The Bill should also require agencies not to alter/delete such data and if they must, then make and retain an evidential record of the computer prior to their alteration, which must be provided to the accused once they are charged.

   At present, nothing in the proposed safeguards prevents an agency from deleting or altering data that an accused might need to prove their innocence, whether the alteration/deletion is done as a by-product of a search, or for concealment, or done purposefully. The common example being altering the date/time stamps needed to show whether or not a particular file has been accessed by the computer's users i.e. that the accused has knowledge of what was in the file or whether they

unknowingly downloaded that particular file co-mingled amongst other files that they actually wanted and viewed.

Note that there have been a number of cases, including one terrorism trial example (see [2014] NSWCCA 303 http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWCCA/2014/303.html), where this was alleged to have occurred.

8. That agencies be required to maintain an audit trail or access log for interception/decryption or for the access process itself. An Access Audit trail should be subject to audit/review by independent authority (not commercial) on regular basis to ensure that access is lawful and aligned with the required audit.

9. The authority of individual applications and telecommunications service providers to outsource or use a third party to meet their obligations under these acts needs close and careful supervision in order to ensure that appropriate controls, documentation and knowledge of such action is maintained.

10. Minimum requirements concerning confidentiality and security clearances should be imposed on persons obligated to provide support.

11. Within Law Enforcement Agencies themselves, the ability to decrypt and access protected data should be strictly controlled and reviewed.

12. Greater clarification is required to distinguish between the circumstances in which the new powers may be invoked, and the scope and nature of those powers once invoked.

13. Considerable care is needed to protect whistleblowers and others with strong personal ethics from the predictable leakages and political interference.

Reviewing the bill

Existing legislative regimens offer an extensive and broad range of authorisations for law enforcement agencies to require assistance of telecommunications and other service providers today. Given that reality, we believe there is no need to expedite this legislation and that more time and consideration should be put into both the wording and need for this bill.

We also believe that this Bill as it stands also has the potential to erode trust in the Australian Government and its agencies, as the governance and accountability processes are obscure. The underlying issue is that in the absence of a Bill of Rights or any constitutional protections is that, unlike all other Anglo-nations, such measures are wide open to abuse without contestability.

Consequently, we believe this Bill would best be put forward as part of a package of wider and more publicly credible governance measures. In the absence of such measures, we believe the Bill as it stands is problematic.

Thank you so much for your time and the opportunity to comment. We're more than happy to discuss the bill with you further. If you'd like to discuss any part of this letter or simply seek further advice on issues of cyber security, please feel free to contact out Director of Corporate Affairs Troy Steer by email at troy.steer@acs.org.au or by phone on 0417 173 740.

Yours sincerely

Andrew Johnson
Chief Executive Officer
Australian Computer Society