Supplementary Submission to the PJCIS Inquiry into the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Dr Chris Culnane and Associate Professor Vanessa Teague
School of Computing and Information Systems, University of Melbourne

Recommendation: Repeal the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, in its entirety, immediately.

We participated in the two rounds of consultation on earlier drafts of the AA Bill, so we are not going to write a long submission this time.

The version of the AA Bill that suddenly appeared on the day it became law was in many ways worse than the drafts to which so many Australians so vigorously objected—it ignored this input almost completely.

We will not give an exhaustive list of everything that needs to be corrected, because we do not believe that minor modifications could address its serious threats to Australian security and freedom. We simply give two examples that show that this legislation is draconian in its provisions and nonsensical in its drafting. It should be repealed in full. Then the democratic assessment of an alternative could begin.

1. The definition of "systemic weakness"

From the very beginning of this debate, the question has been how to guarantee that a law enforcement action targeted against one person doesn't accidentally undermine the security of others. The drafters of the AA Act tried to prevent this by forbidding Technical Assistance Requests, Technical Assistance Notices and Technical Capability Notices from introducing a "systemic weakness."[1] The term was undefined in the draft bill, and extensively discussed during PJCIS hearings, with suggested definitions ranging from the broadly protective "[action that] jeopardizes the information of others," to the very restrictive "weakness that affects a whole system." The version suddenly written into law was even more restrictive:

> *"(317B)* ***systemic weakness*** *means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person."*

This has rightly been described as an abomination. It allows law enforcement to demand modifications that undermine the cybersecurity of millions of people, as long as something less than "a whole class of technology" is affected. It addresses concerns about others' security by simply defining the issue away. Like the Indiana Pi Bill, *which did not pass because the legislators of the time actually listened to a maths professor who happened to be present during the debate*, it simply asserts what the outcome will be irrespective of the constraints of logic.

The extra comment offered in Section 317ZG is inconsistent with the definition.

> *"(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person."*

---

1 Extending the restriction to Technical Assistance Requests was one positive change that was made to the draft bill.

This would have been a good definition if it had been the definition,[2] but as it is, it simply contradicts the definition. There are many actions that jeopardize the security or information of others but do not affect "a whole class of technology," such as targeted malware, or the installation of a keylogger onto a shared computer. It is not clear whether this comment widens the definition (which would be good), or offers inconsistent commentary. Hence it is not at all clear whether a TAR, TAN or TCN may jeopardize the security or information of others.

The Attorney General decides whether a particular action introduces a "systemic weakness" (317WA). The decision must "have regard to," but need not comply with, a pseudo-independent assessment. The process allows the targeted communication provider no way to bring in their own experts or offer their own argument in defence of themselves or the users of their systems. Our recent Attorneys General have not demonstrated the slightest understanding of cybersecurity. Consider Sen George Brandis's effort to protect sensitive datasets from re-identification by making it a crime to demonstrate how weakly the government had de-identified them, or his declaration that "If there are encryption keys then those encryption keys have to be put at the disposal of the authorities."[3] We do not see why an assessment by the Attorney General will be fair or accurate.

2. Compulsory assistance by a person with knowledge of a computer system.

The AA Act makes two mentions of forcing someone with technical expertise to assist in an investigation. The person does not need to be suspected of any crime—he or she simply needs to be suspected of having the privilege and technical expertise to extract some information.

One clause amends the end of Division 2 of Part III of the ASIO Act. It reads

"34AAA Person with knowledge of a computer or a computer system to assist access to data

(1) The Director-General may request the Attorney-General to make an order requiring a specified person to provide any information or assistance that is reasonable and necessary..."

A person who refuses to assist can be jailed for 5 years. A similar provision now added to the Surveillance Devices Act (2004) allows the innocent person to be jailed for 10 years. There is no exclusion for jeopardising the information or security of others.

We would like to know whether any MP or Senator stood up in Parliament and seriously advocated jailing innocent Australian technologists, mathematicians, or engineers for refusing to undermine the security of critical Australian infrastructure.

We are not lawyers, and have heard some more expert legal scholars say that this is probably not the way this clause was intended. If that is the case, it should be repealed and replaced with something that more closely resembles what the MPs of a democracy should support.

Conclusion

These are probably not the only provisions in which substantial damage might be done to Australia's security, or in which innocent people might go to jail for many years. We do not believe the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 deserves to be amended, because there are probably countless other extreme penalties and

---

2 A better definition would include "… jeopardize the security or information of any other…" As pointed out by Dr Paul Brooks, breaking the security of, for example, a critical control system, may do damage without exposing information.

3 https://www.smh.com.au/politics/federal/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html

unintelligible drafting errors. It deserves to be repealed, entirely, immediately. Then perhaps we could have a democratic process for deciding what law to write instead.

Postscript

The definition of "computer" added to the Surveillance Devices Act is just funny:

36 Subsection 6(1) (definition of computer)

computer *means all or part of:*
(a) one or more computers; or
(b) one or more computer systems; or
(c) one or more computer networks; or
(d) any combination of the above.

So "computer" could mean

*"all or part of one or more **computer**s"*

which could mean

*"all or part of one or more (all or part of one or more **computer**s)s"*

which could mean

*"all or part of one or more (all or part of one or more (all or part of one or more **computer** networks)s)s"*

which could mean

*"all or part of one or more (all or part of one or more (all or part of one or more (all or part of one or more **computer** system)s networks)s)s"*

which could go on forever without telling us much about what "computer" means.

It could also be interpreted to mean anything on the same network of networks, which would mean a "computer access warrant" covers anything on the Internet.

Next time the Australian parliament chooses to interfere with the most complex logical systems that have ever been devised, we recommend giving at least one computer scientist the opportunity to read the legislation before it is passed through both houses of parliament.