Submission to inquiry by Parliamentary Joint Committee on Intelligence and Security: "Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018"

Addressed to the Parliamentary Joint Committee on Intelligence and Security.

2019-06-29

Definitions:

the Act: Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

CAW: computer access warrant

DCP: designated communications provider

TAR/TAN/TCN: technical assistance request, technical assistance notice, or technical capability notice (depending on how the acronym is written)

I have several concerns about the Act. As instructed in the call for submissions, I address the following terms of reference in this submission to the Joint Committee.

The threshold, scope and proportionality of powers provided for by the Act

The idea that the government can force Australian people to create or assist in the creation of a weakness in their own technologies is highly disturbing. The Act is overly broad in its reach and is disproportionate in its power, making it a serious threat to digital security and human rights. I identify a few of those issues here.

- The Act shows a serious disregard for the security of our digital devices and infrastructure, rendering every digital thing with any Australian connection as potentially compromised. Given the banning of Huawei and ZTE from Australia's 5G and NBN for security reasons, the Act is utterly hypocritical.
- Contrary to statements of investigating "serious crimes, including terrorism"[1], the threshold for use of TARs/TANs/TCNs and CAWs is any criminal offence with a maximum imprisonment of at least 3 years. The low threshold suggests that the Act is intended to be used routinely for everyday policing rather than to keep Australia safe.
- The "Australia's national economic well-being" objective is vague, has questionable necessity to keep Australia safe and is potentially undesirable. The objective may be used as a pretext to favour pursuits that are in Australia's commercial interests over keeping Australia safe.
- Powers to "add, copy, delete or alter other data" in a computer or communication in transit are far more intrusive than purely a search. In addition to the intrusiveness, such powers also put the security of personal data and digital devices at risk, and are capable of interfering with the proper operation of devices and communications.

1 https://minister.homeaffairs.gov.au/peterdutton/Pages/five-country-ministerial-2017-joint-communique.aspx

Authorisation processes and decision-making criteria

The Act states that a chief officer authorised to approve a TAR/TAN/TCN (issuance, variation or revocation) must be satisfied that the TAR/TAN/TCN is "reasonable and proportionate". I identify the following issues regarding the approval process.

- Independence of the approval decision is highly questionable. The people authorised to approve a TAR/TAN/TCN are closely tied with intelligence and law enforcement agencies who so desperately wanted the powers provided for by the Act.
- Although a TAR/TAN/TCN must have an underlying warrant, a judge who approves a warrant will not see nor be able to challenge what TARs/TANs/TCNs are used to execute the warrant.

The scope of enforcement provisions and the grant of immunities

The Act is a legal minefield that exposes many Australian people to a non-trivial risk of criminal prosecution and imprisonment. I give the following examples.

- Due to the secrecy provisions and the broad scope of "designated communications provider", an electronics or software hobbyist who inadvertently says they have never been served a TAR/TAN/TCN may be committing an unauthorised disclosure.
- Anyone served a TAR/TAN/TCN or an assistance order or is otherwise forced to assist the government must be very careful about how they consult with the government, how they seek legal advice, and what they say and do.
- Anyone served a TAN/TCN or an assistance order or is otherwise forced to assist the government may be charged for non-compliance and may be unable to prove their inability to assist. For example, it may be impossible to prove that seemingly random data is not encrypted data, or to prove non-possession of a password or cryptographic key. The Act worsens this by raising some non-compliance penalties.

Interaction with intelligence agencies' other powers

The mandatory data retention law provides for some protections for journalists. However, the Act makes no mention of "journalist" or "journalism", and allows for access to data about journalists even in the absence of a special journalist warrant[2]. Combined with the secrecy provisions and lack of judicial review, the Act presents a serious threat to journalism and press freedom.

The combination of powers provided for by the Act and other surveillance laws (eg: the data retention law) form a panopticon that is capable of surveilling every aspect of Australians' lives, now including encrypted communications. Far from being "not absolute", privacy is almost non-existent. People being unable to read, associate, talk, express, report, shop or move around without always being spied on has a chilling effect on society that amounts to mass erosion of both human rights and democracy[3,4,5].

2 https://www.commsalliance.com.au/Documents/releases/2019-media-release-2

3 https://www.un.org/en/universal-declaration-human-rights/index.html

4 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

5 https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/

Interaction with foreign laws

I identify the following issues in relation to the Act allowing the government to use the new powers to cooperate with foreign countries.

- The Act allows the government to assist a foreign country in investigation of an offence punishable by torture, death penalty or other serious human rights violation. Australia should not take part in facilitating those kinds of human rights violations.
- The Act allows the government to assist a foreign country in investigation of an offence, even if the foreign offence is considered lawful conduct or minor under Australian law. Australia should not assist in the investigation of (for example) homosexual activity that occurs under foreign law.

Impact on industry and competitiveness

Soon after assent of the Act, reports of Australian industry raising economic concerns, losing customers or relocating away from Australia have emerged[6,7,8]. As users shy away from technologies with any Australian connection[9], Australian people will also lose opportunities to work in technology industries of foreign countries due to fear by foreign companies that Australian people are a security risk[10]. The impact on industry extends to career choices of prospective technology workers and STEM education.

Technology providers who put privacy, security and their customers first and will not compromise their values would feel compelled to shut down or relocate away from Australia. Australia should be doing what it can to retain technology providers who uphold high standards of integrity and morality, not drive them away from Australia. The Act effectively criminalises Australian people to develop and use secure technologies.

Reporting obligations and oversight measures

While I understand the strategic importance of not revealing operations in detail and during execution, the government should not be beyond reach of accountability. The Act has secrecy provisions that protect TAR/TAN/TCN information, making the provision of sufficient accountability and oversight more difficult.

The Act allows a DCP to disclose statistics about TARs/TANs/TCNs, but only numbers of each that fall in a period of at least 6 months and without further information of any kind. The Home Affairs Minister's report on use of TARs/TANs/TCNs is required only annually, does not require the breakdown of statistics by issuing agency, and allows the omission of foreign offences and less serious offences.

With only highly aggregated and untimely TAR/TAN/TCN statistics, Australian people will have limited sense of whether or not the Act is justified and effective. Combined with the lack of judicial review for approval of TARs/TANs/TCNs, Australian people will have minimal ability to ensure sufficient oversight and accountability.

6 https://www.itnews.com.au/news/fastmail-loses-customers-faces-calls-to-move-over-anti-encryption-laws-519783

7 https://www.smh.com.au/politics/federal/companies-no-longer-comfortable-storing-data-in-australia-microsoft-warns-20190327-p517yz.html

8 https://www.reddit.com/r/sysadmin/comments/ag5of9/australias_assistance_and_access_bill/ee3vlbq/

9 https://branchfree.org/2019/02/28/paper-hyperscan-a-fast-multi-pattern-regex-matcher-for-modern-cpus/

10 https://www.itnews.com.au/news/mozilla-may-treat-aussie-staff-as-insider-threats-to-code-base-519793

Recommended changes to the Act:

- Explicitly state that a TAR/TAN/TCN can only target technologies a DCP provides as a service, and not (for example) operational processes or procedures.
- Explicitly state that when it is a company who provides a technology that the company be defined as the DCP and not any individual of the company.
- Permit a DCP to reverse anything done as part of complying with a TAR/TAN/TCN (eg: promptly close up weaknesses), after its underlying warrant has expired.
- Require that the government confidentially disclose to a DCP all weaknesses that were exploited as part of a TAR/TAN/TCN (eg: so that the DCP can work on security fixes) that are not being exploited by another TAR/TAN/TCN in effect and served to the same DCP, after a period of 6 months and after its underlying warrant has expired.
- Permit a DCP to disclose all weaknesses that the government has disclosed to the DCP (eg: so that the DCP can announce fixes in a Changelog), excluding any information about their connections to any TAR/TAN/TCN.
- Raise the threshold of use of the powers provided for by the Act to exclude less serious offences, and limit the kinds of offences to only offences that pose a genuine and serious threat to Australian people.
- Remove "Australia's national economic well-being" as a justification for use of powers provided for by the Act.
- To avoid the loose "if necessary to achieve that purpose" justification, explicitly specify the kinds of actions as part of execution of a CAW or search warrant that are permitted to "add, copy, delete or alter other data", and ensure those are written in warrants.
- Require judicial review for all TAR/TAN/TCN approvals.
- Explicitly require proof beyond reasonable doubt that a TAN/TCN or assistance order recipient is able to execute the order before they can be charged for non-compliance.
- Explicitly require a special journalist warrant or special approval to target a journalist for any TAR/TAN/TCN or CAW that targets a journalist.
- Prohibit the use of powers provided for by the Act towards investigation of offences that may be punishable by torture, death penalty or other serious human rights violation.
- In relation to foreign offences, limit the use of powers provided for by the Act to that of investigations of criminal offences of a foreign country that have a comparable criminal offence under Australian law and that satisfy the punishment threshold (currently set at 3 years imprisonment) under the laws of both countries.
- Increase the frequency and breakdown of information that the Home Affairs report provides for, with breakdowns about numbers of TARs/TANs/TCNs by agency and by offences of all kinds including foreign offences (not only "serious Australian offences").

- Add a criminal offence, comparable in seriousness to unauthorised disclosure of TAR/TAN/TCN information, for issuance or variation of a TAR/TAN/TCN that lacks an underlying warrant or is not properly approved (an unlawful TAR/TAN/TCN).
- Permit the disclosure of an unlawful TAR/TAN/TCN, particularly the details of its issuance or variation and grounds for it being unlawful, excluding any details that may jeopardise any related investigation that may exist.

This submission should not be taken as my endorsement of the Act nor its process of assent. The rushed process that led to the Act being assented undemocratically denied Australian people the right to discuss the threats that we face[11,12,13].

Above all of the above recommendations, I recommend that the Act be repealed, and that the government approach Australian people to have an honest and sincere discussion about human rights, digital security and keeping Australia safe.

---

11 https://www.eff.org/deeplinks/2018/09/australian-government-ignores-experts-advancing-its-anti-encryption-bill

12 https://digitalrightswatch.org.au/2018/12/06/australian-parliament-ignores-overwhelming-evidence-against-encryption-bill/

13 https://alp.fail/