April 2020

Dr James Renwick CSC SC
Independent National Security Legislation Monitor
12/174 Phillip St
Sydney, NSW 2000
Phone: (02) 9232 8545

By email: INSLM@inslm.gov.au

Dear Dr Renwick,

REVIEW OF THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018

Thank you for inviting Access Now as an expert witness to present our work and concerns regarding *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* (TOLA) at the February 20th, 2020 hearing held in Canberra.[1]

Access Now has been actively engaged in consultation of TOLA since early 2018 before the full text was introduced. We appreciate the continued opportunity to highlight the human rights challenges posed by the powers enshrined in this legislation. In our letter to you in October 2019, we took the opportunity to highlight our previous work and submissions we made to the four Parliamentary Joint Committee on Intelligence and Security (PJCIS) consultations which have preceded your inquiry.

In support of the testimony we provided in Canberra earlier this year, we further submit this letter to your inquiry, detailing some of the points which came up during the inquiry, and highlighting the links to external resources and documents which we cited.

Necessity and proportionality of measures

We are cognisant that end-to-end encrypted communications pose a disruption to some of the working methods of law enforcement and intelligence agencies, however, the security of those channels is essential for the protection of privacy of everyone who uses the internet.[2]

[1] https://www.inslm.gov.au/current-review-work
[2] While often overlooked, prior to the 1990s, law enforcement and intelligence services had a limited scope of activities often tied to data they could secure by electronic means within active human measures/intervention. The digital environment has changed that so in terms of investigative practices that encryption is impacting are those developed between 1999 to 2010/11.

The solution should not be to compromise the security of communications channels as is currently possible through Technical Assistance Notices (TANs) or Technical Capabilities Notices (TCNs) under TOLA. As stated in our testimony, we believe that the necessity and proportionality of those measures has NOT been demonstrated, as other means have not been properly explored or reported on by the government;

While end-to-end encryption poses a barrier to communications interception or remote access, the data/content does exist unencrypted and is therefore susceptible to alternate means of physical or digital surveillance conducted with due process for lawful ends.

In many jurisdictions, governments have sought to utilize either traditional surveillance (microphones or cameras) or "government hacking" to take advantage of this access, which lead us to publish *A Human Rights Response to Government Hacking* in 2018.[3] Physical surveillance is subject to judicial oversight and warrants, which means the threshold for deploying is much higher than what is currently prescribed under TOLA for TCNs – the approval of the Attorney General.

In their paper *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications,* Schneier, Landau et al lay out all options for "privileged access" to encrypted communications, highlighting the impossibility of balancing security and privacy as is often proposed by law enforcement and intelligence agencies.[4] In our February testimony we further referenced the 2018 paper by Orin S. Kerr and Bruce Schneier entitled *Encryption Workarounds* in which they go over alternate methods (as mentioned above) as well as the potential overreach that such privileged access often embodies.[5]

Additionally, as users increasingly connect to more online/connected services, critical questions must be posed whether the mere existence of data or content should presume law enforcement access. In many cases if these capabilities were to be built by and for law enforcement – the hypothetical that was used in the inquiry hearing was if they would build their own social media style surveillance with clear ties across networks and user behaviors – people would be rightfully outraged at the disproportionate violation of privacy. Private companies operate with a different social license than government agencies do, though both bodies have to respect the right to privacy.

Individual's rights

There is a disproportionate focus on the government-company relationship in TOLA, often sidestepping – if not entirely overlooking – who guarantees and sits responsible for the protection of individual's rights. Given the absence of federal-level protection of privacy and/or data protection in Australia, and the absence of a requirement for judicial warrant or even an *ex post* notification to the individual, the powers enshrined in the legislation fully strip individuals' rights to a fair trial, appeal, and remedy.

---

[3] https://www.accessnow.org/cms/assets/uploads/2016/09/Gov-Hacking-Three-Pager.pdf
[4] https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf
[5] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033

This is further compounded by guaranteeing that service providers (DCPs) cannot be sued by individuals for compliance with orders under TOLA. In this regard, the Act ensures cooperation by the service providers by fully blocking any individual challenge, resulting in the removal of a key accountability and enforcement channel for individual users. It absolves the provider from their legal responsibilities under international law and removes any leverage or guarantee that the provider would act in line with legal responsibility, let alone on their behalf.

During the hearings, an argument was made by a Home Affairs representative that TARs do not require judicial approval because if the company does not agree with the content of the request they may choose not to respond. Given the above mentioned removal of legislative remedy between the individual and the company, there is no reason to believe that such discretion would be exercised.

While the appropriate agencies will approach private entities in the course of their investigation, it is a gross deficiency of TOLA that no representation or challenge is left to the individual. We firmly believe that individuals have a right to due process and should be notified, concurrently or at the very least *ex post* in extremely exceptional circumstances, that they were subject to the powers enshrined in the legislation. Various interpretations of this are present in legislations abroad, such as with the USA FREEDOM Act Delayed Notice Search Warrants which seek to allow agencies access without tipping off a suspect, only issuing notice (as with a regular Warrant) after the bulk of the investigation.[6]

Privatized enforcement

In our testimony to this point, we referenced the recent Advocate General opinion delivered to the Court of Justice of the European Union (CJEU) on Case C-623/17 which is examining investigative powers granted under the UK Investigatory Powers Act.[7] In his opinion, the AG takes the position that privatized enforcement – relying on private entities to hold, collect or police data and content – is not compatible with EU law, stating: "*the notion of national security, which is the sole responsibility of each Member State… cannot be extended to other sectors of public life that are, to varying degrees, related to it*." Essentially advising that EU states cannot delegate their responsibility on national security to private actors.

Evaluation and reporting

Due to the gag orders which are imposed on service providers if they are approached under TOLA, the government's own reporting on the use and scope of the Act must be more than symbolic and not subject to discretion of any person or entity. As suggested in the civil society submission to PJCIS in June 2019:[8]

---

[6] https://www.justice.gov/sites/default/files/dag/legacy/2008/10/17/patriotact213report.pdf
[7] http://curia.europa.eu/juris/celex.jsf?celex=62017CC0623&lang1=en&type=TXT&ancre=
[8] https://digitalrightswatch.org.au/wp-content/uploads/2019/07/190701-Submission-to-the-Review-of-the-Telecommunications-and-Other-Legislation-Amendment-Assistance-and-Access-Act-2018.pdf

Put in place annual reporting requirements on the part of the Attorney General in respect of powers exercised under Sch 1 and Sch 2 of the Act as they relate to the Telecommunications (Interception and Access) Act 1979. Such reporting requirements exist under s 94 of the Australian Security and Intelligence Organisation Act for powers used by ASIO, including under the Telecommunications Act. The Attorney General should be legislatively required to collate all instances where the powers under Sch 1 and Sch 2 were exercised (across all agencies) and table the report in parliament each year.

Furthermore, there must be a consistent and overarching obligation to consider community expectations of privacy and the security of digital infrastructure in the issuing of TARs, TANs, and TCNs. As stated in our testimony, we would recommend that a technical opinion and assessment is integrated into the necessity and proportionality weighing mechanism under 317RA and 317ZAA, possibly through an independent technical expert panel as was discussed during the hearings that day.

Closing remarks

Thank you for extending us the opportunity to provide evidence to your inquiry into the Act. We look forward to the final report you will be presenting to the Parliament later this year.

If we can provide any further evidence, please do not hesitate to contact us.

Regards,

Lucie Krahulcova
Policy Analyst, Australia and Asia Pacific
Access Now