

Submission to PJCIS

on the Review of the

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

1 July 2019

Australian Civil Society Coalition

This submission is endorsed by:

Digital Rights Watch
Blueprint for Free Speech
Human Rights Law Centre
NSW Council for Civil Liberties
Queensland Council for Civil Liberties
Liberty Victoria
Access Now
Electronic Frontiers Australia
Future Wise

Australian Civil Society Coalition

Introduction

The coalition of civil society organisations that have endorsed this submission are grateful for the opportunity to provide further input to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA).

We have provided significant input to the process for considering the bill before it was passed, including coordinating nearly 15,000 submissions from the public (via Digital Rights Watch) and making a lengthy submission to the PJCIS. Our position remains as it was then: that PJCIS should wholesale reject this bill (now law). The Act should be repealed in its entirety. We are deeply concerned by the powers contained in the Act, and the serious implications for human rights and democratic governance.

We are very concerned about the substandard and unnecessarily rushed parliamentary process that led to this law being passed. Many parliamentarians simply could not have had time to explore the numerous concerns they may have had about the impact of this law on the personal privacy and digital security of their constituents and the detrimental impacts on Australian industry.

We think this review is an opportunity to fix these errors. That ought to involve full repeal. To do so would be in line with the recommendations by a broad range of organisations, companies and individuals who expressed concerns about the bill before it passed.

That said, we also understand that further specificity in articulating our concerns may be of use to the PJCIS, and as such, we present the following short submission.

We note the terms of reference to this review and have confined our comments to the relevant provisions of the Act, as they apply to the *Telecommunications (Interception and Access) Act 1979* (TIA), notwithstanding that our objections remain broader than the scope of this review.

Context

We note the following events that have taken place since the passage of the Act:

- Raids on journalists: there have been two recent raids by journalists (News Ltd and ABC) that have been conducted reportedly involving powers conferred by TOLA. We note that according to John Lyons, Executive Editor ABC News and ABC Head of Investigative Journalism, the warrant issued in relation to the ABC authorised the relevant officer to ‘to add, copy, delete or alter other data in the computer or device.’

These are powers that became available as a result of amendments to the *Crimes Act 1914* by TOLA. We are aware that this amendment technically falls outside the scope of this review. However, this context is worth noting given the serious public concern generated by these raids. It comes as no surprise to critics of the increased powers granted to national security agencies over the last decade that this context has given rise to a situation where those powers are directed at journalists and sources associated with reporting that is in the public interest.

- Comments by NSW police: at an event hosted by the McKell Institute on 4 March 2019, Arthur Kopsias, a serving member of the NSW police force, indicated that the NSW Police were not meaningfully consulted about TOLA prior to the bill be tabled before parliament. This revelation suggests that one of the primary justifications for TOLA, namely that investigations of serious crimes by law enforcement were being hampered by widespread encryption, was not informed by the experience of state police bodies that deal with these issues on a daily basis. This revelation, together with the way in which the Bill was rushed through Parliament thereby avoiding proper scrutiny and necessary consideration, rings alarm-bells. We are deeply concerned that the unprecedented new powers given to agencies remain at large, without anything near appropriate checks and balances.

Recommendations

We note that TOLA refers to TIA on a number of occasions, and specifically in section 317ZH which provides limits on the use of Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs).

In our opinion, given the context cited above and our substantive submissions to multiple reviews of TOLA, the following matters ought to be of urgent priority for the PJCIS:

- **Repeal** of TOLA in its entirety, including all amendments to TIA.
- The acknowledgement of the urgent need for the introduction of an **enforceable federal human rights framework**. Without this, Australia remains the weak link in relation to the Five Eyes intelligence sharing network, and its citizens vulnerable to over broad legislative amendments that undermine fundamental rights.
- Enshrine robust **protections for whistleblowers** who expose wrongdoing in relation to powers exercised under TOLA. These protections could be dealt with by an extension of the *Public Interest Disclosure Act* to apply to requests or notices issued under Sch 1 or Sch 2, or similar provisions. This has become particularly urgent in light of the recent raids on journalists.

- Introduce a **warrant-based system** with judicial consent to TANs and TCNs. Such a reform would be in line with similar legislation abroad, and community expectations. Without independent review, overreach and abuse is likely, as we have seen in relation to the metadata retention regime under TIA generally. Indeed, the greater concern is that it will not be possible to prevent or even identify overreach and misuse.

The significance of this requirement has been recognised by the European Court of Human Rights in *Big Brother Watch & Ors v United Kingdom*, where the court said at [309]:

“[S]ince the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.”

This ought to include a requirement such that any request for voluntary assistance, including a TAR, cannot be made in circumstances where obtaining such information would require a warrant, to avoid voluntary assistance being used to circumvent any warrant regime.

- Legislate a requirement that any capabilities or tools developed as a result of a TAR, TAN or TCN be **restricted to use only pursuant to a judicial warrant**. When that warrant is no longer in force, the recipient of the TAR, TAN or TCN should be notified appropriately and permitted to take any steps to address the impacts of the TAR, TAN or TCN as they see fit. Put differently, there should be a statutory prohibition imposed on all agencies (located in Australia or elsewhere) using any technical capacity, capability or knowledge generated as a result of a TAR, TAN or TCN for a purpose other than pursuant to the original warrant or authorisation. This is justifiable for the protection of public safety and cybersecurity. Without such a provision the effectiveness section 317ZH is largely undermined as it applies to the *Telecommunications (Interception and Access) Act 1979*.
- Amend TOLA to **close the loophole** that currently allows agencies to use TOLA powers to access journalist metadata without a warrant, thereby undermining the journalist information warrant process in the TIA.

Under the TIA, access to a journalist’s metadata is only available via a journalist information warrant. This warrant process is woefully inadequate as it is done in secret, and the journalists and their employers will never know that their metadata has been accessed, or have the chance to challenge that access. Nonetheless, the warrant

process provides some protection in the form of third party assessment, inadequate though it is, and that protection is undermined by TOLA.

TOLA provisions in relation to this are extremely vague, complex and unclear. At first reading, section 317ZH(1) seems to preserve the warrant protection provided in other Acts. Read on its own, it would suggest that authorities cannot use TOLA to get access to metadata if access to that data would require an authorisation or warrant under the TIA Act.

However, sections 317ZH(4) and (5) then negate and undermine that protection. Those sections suggest that any act or thing can nonetheless be requested under TOLA if it would “assist in, or facilitate, giving effect to a warrant or authorisation under a law of the Commonwealth, a State or a Territory.” So it would seem that a request for technical information (including a journalists’ metadata) under TOLA can be made so long as it would assist in, or facilitate the giving of effect to a warrant or authorisation otherwise provided, for example other warrants and authorisations that might be made under the TIA Act or the *Telecommunications Act*.

Given the tenuous protection for press freedom in Australia, highlighted by the raids on news outlets recently, it is essential that this loophole be closed.

- Address the problems with the definition of ‘**systemic weakness**’, ‘**systemic vulnerability**’ and ‘**target technology**.’ The current definitions are unclear and offer minimal substantive protection. We support the amendments proposed by Labor and passed by the Senate in February 2019. We also submit that the limitation provided in s 317ZG, if raised by a recipient of a TAR, TAN or TCN, should create a rebuttable presumption that the limitation applies. That is, the effect of the provision would be to shift the burden of proof to the person issuing the request or notice to show that it does not require the recipient to implement or build a systemic weakness.
- Introduce 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.
- 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.