Human Rights Law Centre

DIGITAL RIGHTS WATCH

Submission to the Independent National Security Legislation Monitor

review of the

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

13 September 2019

info@digitalrightswatch.org.au
PO Box 1426 Fitzroy Nth VIC 3068
digitalrightswatch.org.au
ABN 90 509 129 914

Introduction

Digital Rights Watch (DRW) and the Human Rights Law Centre (HRLC) are grateful for the opportunity to provide a submission to the Independent National Security Legislation Monitor (INSLM) review of the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (TOLA). This submission has been drafted on behalf of both organisations.

We have provided significant input to the process for considering TOLA as a bill before it was passed, including coordinating nearly 15,000 submissions from the public (coordinated by DRW) and making a lengthy submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS)[1].

Our position remains as it was then: that the INSLM should wholesale reject this Act, and TOLA should be repealed in its entirety. We are deeply concerned by the powers contained in TOLA, and the serious implications for human rights and democratic governance.

We remain 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 impacts of this law on the personal privacy and digital security of their constituents and the detrimental impacts on Australian industry.

We would welcome INSLM taking the opportunity presented by this review as an opportunity to fix these errors, by presenting a recommendation of 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 INSLM, and as such, we present the following short submission.

Context

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

- Raids on journalists: in 2019, there have been two 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

[1] Digital Rights Watch and Civil Society submission to PJCIS inquiry into TOLA, 2018: https://digitalrightswatch.org.au/2018/10/12/submission-to-pjcis-on-the-assistance-and-access-bill-2018/

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. There was 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 welcome your review into the operation, effectiveness and implications of amendments made by TOLA. We confirm that we do not believe TOLA contains appropriate safeguards for protecting the rights of individuals. TOLA is not an appropriate or proportionate response to any threat of terrorism or threat to national security. We are not of the view that the necessity of TOLA has been sufficiently justified by the relevant stakeholders.

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 INSLM:

- **Repeal** of TOLA in its entirety.

- The acknowledgement of the urgent need for the introduction of an **enforceable federal human rights framework or Charter of Human Rights**. 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 2013* 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. We maintain reservations about the *Public Interest Disclosure Act 2013*,[2] but an extension of its application nonetheless remains urgent and necessary.

- Introduce a **warrant-based system** requiring judicial consent to Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (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 the metadata retention regime contained in the *Telecommunications (Interception and Access) Act 1979*. 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*[3], 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."

  TARs are voluntary, but this requirement ought to similarly apply. Any request for voluntary assistance should not be made in circumstances where obtaining such information would require a warrant, to avoid voluntary assistance being used to circumvent any warrant regime.

---

[2] Human Rights Law Centre submission to PJCIS inquiry into TOLA: https://static1.squarespace.com/static/580025f66b8f5b2dabbe4291/t/5d3e93096eae2d0001a6f2d9/1564381967766/FINAL+HRLC+submission+to+PJCIS+inquiry+law+enforcement+and+press+freedom....pdf

[3] https://hudoc.echr.coe.int/eng?i=001-186048

Judicial consent should also be required for any variation of a TAR, TAN or TCN.

- 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 *Telecommunications (Interception and Access) Act 1979*.

  Under the *Telecommunications (Interception and Access) Act 1979*, 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 *Telecommunications (Interception and Access) Act 1979*.

  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 *Telecommunications (Interception and Access) Act 1979* or the *Telecommunications Act 1997*.

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, the security of digital infrastructure and press freedom** 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 TOLA. Such reporting requirements exist under s 94 of the *Australian Security and Intelligence Organisation Act 1979* for powers used by ASIO, including under the *Telecommunications Act 1997*. Current reporting requirements are minimal and the Home Affairs Minister is empowered to delete information from the Commonwealth Ombudsman's reports to Parliament about the operation of encryption legislation. 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.

- **Repeal the provision that compels a person with knowledge of a computer or a computer system to assist** with providing access to a computer (s 114, the new s 64A of the *Surveillance Devices Act 1999*). This power is too broadly defined and vague, and potentially infringes a range of human rights. It is essential to introduce limits on the use of this power, clarify what they can be required of someone and introduce a

requirements to consider and protect the public interest in security of digital infrastructure.

- **Increase the thresholds** for using powers in the legislation such that the offence must be a serious offence, punishable by imprisonment of life or for maximum period of at least 7 years. The current threshold at which agencies may engage TOLA powers is far too low. The powers can be used to investigate serious offences, defined to mean crimes that carry a penalty of at least three years imprisonment. This captures relatively innocuous offences such as making a prank call (which attracts a maximum three year sentence under division 474.17 of the *Criminal Code Act 1995*). The three year threshold is out of step with the *Telecommunications (Interception and Access) Act 1979* which already defines "serious offence" as an offence punishable by imprisonment for life or for a period, or a maximum period, of at least seven years. The meaning of a serious offence should be the same for TOLA.

- **Strengthen the process** for consultation with industry in advance of issuing a TAR, TAN or TCN. Currently the assessor process under ss 317WA and 317YA only applies to TCNs and are otherwise limited. Such a consultation and assessment process ought to apply to all TARs, TANs or TCNs to determine whether there may be a risk of a contravention Section 317ZG. This could include for example, the appointment of an independent expert to provide an opinion in relation to the TAR, TAN or TCN. The recipient of a TAR, TAN or TCN should be given the opportunity to challenge the content of the request or notice, participate in the process of obtaining an opinion from an independent expert, and negotiate the terms of any implementation. Introducing a statutory process would minimize the potential for abuse.