AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

# Independent National Security Legislation Monitor

## Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

November 2019

# Table of Contents

# Introduction

The Australian Criminal Intelligence Commission (ACIC) is Australia's national criminal intelligence agency, uniquely equipped with intelligence, investigative and information delivery functions. The ACIC works to identify new and emerging serious and organised crime threats and criminal trends, to create a national strategic intelligence picture across the spectrum of crime, to fill intelligence and knowledge gaps and to share information and intelligence holdings to inform national and international responses to crime. The ACIC undertakes its work in partnership with others.

The ACIC welcomes the opportunity to make a submission to the Independent National Security Legislation Monitor's (INSLM) review of *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act). This submission addresses the ACIC's implementation and use of the powers afforded by the TOLA Act, the persistent threat environment in which the ACIC and other intelligence and law enforcement agencies operate and the critical need to ensure the utility of the TOLA Act is not diminished. The contents of this submission are unclassified and suitable for public release.

## Role and function of the ACIC

The ACIC is established in legislation by the *Australian Crime Commission Act 2002* (Cth) (ACC Act), with supporting legislation in each of the states and territories. Functions of the agency as set out under section 7A of the ACC Act include:

- to collect, correlate, analyse and disseminate criminal information and intelligence
- to maintain a national database of criminal information and intelligence
- to provide and maintain national information capabilities and services to support policing and law enforcement
- to provide strategic criminal intelligence assessments and advice on national criminal intelligence priorities
- to conduct investigations and intelligence operations into federally relevant criminal activity (principally serious and organised crime) when authorised by ACIC Board
- to provide nationally coordinated criminal history checks.

## ACIC governance and oversight mechanisms

The ACIC is subject to a stringent oversight regime which includes the Minister for Home Affairs, state and territory police ministers (as represented by the Inter-Governmental Committee on the Australian Crime Commission), the Parliamentary Joint Committee on Law Enforcement, the Australian Commission for Law Enforcement Integrity, the Board of the ACIC, the Commonwealth Ombudsman, and the Australian National Audit Office. The ACIC is also accountable to the courts for the lawful and appropriate use of its powers.

As a Commonwealth statutory authority the ACIC also has responsibilities and obligations under the *Public Service Act 1999* (Cth) and the *Public Governance, Performance and Accountability Act 2013* (Cth). The ACIC is subject to further parliamentary scrutiny for example by the Senate Legal and Constitutional Affairs Committee, which has general portfolio responsibility for law enforcement, via the Senate Estimates process and general inquiries.

Additionally, the Government's intent is that the ACIC also fall under the oversight of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Inspector-General of Intelligence and Security (IGIS) in accordance with the Office of National Intelligence Act and

recommendations made by the 2017 Independent Intelligence Review. This is in line with ACIC's inclusion in the National Intelligence Community.

The ACIC also acknowledges the essential role the INSLM plays in providing an additional avenue for independent oversight. Reviews such as this one are another example of the kind of the Commonwealth mechanisms in place to ensure ACIC's activities and its use of legislation remain effective, proportionate, ethical, legal, and in-keeping with community expectations.

# Enduring transnational, serious and organised crime exploitation of encryption

As noted in the ACIC's Organised Crime in Australia 2017, the majority of serious and organised crime activities are enabled, to a large extent, by the use of technology. For example, ACIC intelligence reveals that high-end encrypted smartphones continue to be preferred by serious and organised crime groups to reduce the visibility of their activities to law enforcement. Multiple outlaw motorcycle gangs and other serious and organised crime groups use particular deliberately encrypted communications devices and software applications as their primary means of communication, due to the content protection features available on these devices and applications.

The ACIC conducts work to identify emerging technologies and vulnerabilities, inform policy development, and formulate disruption strategies targeting serious and organised crime's exploitation of encrypted communications. However, criminals are creative early adopters of new technologies and methods meaning that ACIC needs to be able to adapt swiftly. Modern legislation that enables this versatility, like the TOLA Act, is therefore vital to ACIC's ongoing effectiveness in a dynamic operating environment.

The ACIC would welcome the opportunity to provide a classified briefing to the INSLM outlining some of the contemporary emerging threats and trends relating to the use of encryption technologies.

# ACIC implementation of the TOLA Act

As Australia's national criminal intelligence agency, the ACIC's use of the TOLA Act is conducted in a strategic and targeted manner to gather intelligence in relation to ACIC Board authorised Special Investigations or ACIC Special Operations.

The ACIC is committed to ensuring that powers are used in a measured and considered way. As such, since implementation of the TOLA Act, the ACIC has been dedicated to ensuring as a first priority that appropriate internal legal advice, governance, accountability and training processes are in effect for the new regime. As part of this process, assisted by guidance material provided by Department of Home Affairs and other agencies, the ACIC has been working to update and develop appropriate templates and processes, training programs and internal procedures to ensure all relevant officers are aware of the scope of lawful use of the TOLA Act and their obligations under the Act, as appropriate opportunities arise. While much of this internal guidance material is classified, the ACIC would welcome the opportunity to expand privately to the INSLM on the implementation steps taken by the agency if appropriate.

# Operational intelligence collection benefits of the TOLA Act

The TOLA Act introduced three main categories of new powers for the ACIC, amongst other agencies:

1. Industry Assistance Measures (TARs, TANs and TCNs) within the *Telecommunications Act 1997* (Telco Act)
2. Computer Access Warrants (CAWs) in the *Surveillance Devices Act 2004* (SD Act), and
3. Enhanced search warrant powers under Part IAA of the *Crimes Act 1914* (Crimes Act).

## Industry Assistance Measures - Schedule 1

Schedule 1 of the TOLA Act provides the ACIC with an avenue to collaborate with industry to secure critical assistance to more efficiently gather intelligence to disrupt serious and organised crime. The comprehensive framework provides an extension to existing relationships with industry to engage and ensure requests and notices are reasonable, proportionate and technically feasible.

The ACIC is proud to have positive relationships of trust with many of Australia's major telecommunications companies. As a result of this trust, most of these private entities are proactive in collaborating with ACIC and our partners in the voluntary manner facilitated by Technical Assistance Requests. However, despite this voluntary assistance, the TOLA regime's provision of the mandatory Technical Assistance Notices and Technical Capability Notices are still essential mechanisms for both ACIC and our private sector partners. For one, some telecommunications companies are reassured by the fact that these mandatory notices often provide them with the legal indemnity to perform tasks they would otherwise not feel comfortable performing voluntarily, such as allowing a Commonwealth agency to use their capabilities for a law enforcement purpose. Additionally, Technical Capability Notices give the ACIC and other Commonwealth law enforcement agencies the option to compel telecommunications companies to install or build capabilities they would otherwise have no commercial incentive to establish. Schedule 1 of the TOLA therefore provides the structure for a mature and accountable collaborative relationship between industry and government agencies that is appropriate for the modern operating environment.

The ACIC notes the non-disclosure requirements as defined in section 317ZF of the *Telecommunications Act 1997* in relation to Technical Assistance Requests, Technical Assistance Notices and Technical Capability Notices. The ACIC would welcome the opportunity to provide additional information privately to the INSLM, if appropriate, in relation to potential scenarios in which use of Schedule 1 is anticipated.

## Computer Access Warrants - Schedule 2

Computer access warrants, as afforded by the TOLA Act, are a key covert intelligence collection tool for the ACIC. They are critical not only for preserving information and evidence but also for improving the safety of operational staff by complementing existing warrant powers afforded by the Surveillance Devices Act. Computer access warrants allow ACIC officers to search the content of electronic devices belonging to major criminal targets. The amendments implemented by the TOLA Act remain necessary to ensure these warrants continue to be operationally effective whilst appropriately limiting the intrusion of individuals' privacy. Where computer access warrants have been used, they have been an important enabler or counterpart to other measures available to us such as coercive examinations. This is reflective of ACIC's systematic approach to exercising its extraordinary powers, whereby measures are deployed in concert to ensure that our officers remain

safe, that our investigations and operations remain highly targeted, all whilst minimising the potential of our activities to inadvertently affect the community.

Since 2018, the ACIC has obtained, through appropriate judicial authority, the issuing of **three** computer access warrant relating to a transnational serious and organised crime drug investigation. The ACIC would welcome the opportunity to provide the INSLM with further detail in a private briefing. Since the establishment of the TOLA Act regime in 2018, ACIC has taken time to carefully implement policies and procedures to ensure the use of computer access warrants is aligned with appropriate oversight and is operationally proportionate. As a result, we expect the number of computer access warrants sought to increase over time now that we have established this internal framework of policies and procedures.

### Enhanced Search Warrants - Schedule 3

The amendments to the Crimes Act introduced by Schedule 3 of the TOLA Act enhance the ability of the ACIC and other criminal law enforcement agencies to collect evidence from electronic devices found during a search warrant. Specifically, these amendments modernise the existing search warrant powers and assistance orders to keep pace with contemporary technology such as smart phones and complex communications systems.

## Ongoing necessity and proportionality to the TSOC threat

Organised crime in Australia is proficient and enduring. It is transnational in nature, technology enabled and increasingly functions as a business: employing professionals; outsourcing key activities such as money laundering; diversifying into multiple criminal markets; and developing strong, consistent revenue streams through involvement in comparatively low-risk activities.

Geographic boundaries no longer restrain criminal networks. Increasing access to and uptake of Internet-enabled technologies provides serious and organised crime groups with the ability to target thousands of Australians simultaneously from anywhere in the world whilst maintaining a high degree of anonymity. The highest threat targets have the skills, knowledge and resources to remain insulated from law enforcement and intelligence efforts and are increasingly aware of or hold a well-founded suspicion about investigations being conducted.

The evolving nature of organised crime and its dynamic exploitation of technology will persistently test the effectiveness of Australia's law enforcement and intelligence legislation. This is why amendments and changes to existing laws, such as those introduced by the TOLA Act are a necessary and proportionate response to the threats we face. ACIC is of the view that all the powers afforded to it by the TOLA Act are a sensible, rational and necessary given the context in which the ACIC operates. This is because the TOLA regime ensures that ACIC's search and surveillance powers in the cyber domain are equivalent to the existing powers ACIC has in the psychical domain. As the INSLM has noted, *"cyberspace should be subject to the same rules as the physical world, unless there are powerful reasons to treat it differently,"*