AFP
AUSTRALIAN FEDERAL POLICE

Parliamentary Joint Committee on Intelligence and Security

Review of the Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 (TOLA)

6 August 2020

Submission by the Australian Federal Police

Introduction

1. The Australian Federal Police (AFP) welcomes the opportunity to make this supplementary submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA).

2. The AFP notes the Department of Home Affairs has made a submission and supplementary submission to this inquiry, on which the AFP was consulted. We offer the following operational context on the AFP's use of powers introduced by TOLA from a law enforcement perspective, to assist the Committee's consideration of the necessity and proportionality of TOLA.

3. As noted in our previous submissions and appearances before this Committee, and in the INSLM review of TOLA, the tempo and complexity of the criminal threat environment is ever evolving with increasing use of technology by criminal groups and their networks, to facilitate and obfuscate criminal conduct. TOLA provides an essential framework to strengthen the AFP's ability to overcome technological impediments to lawful access to digital content, where necessary and appropriate.

4. The AFP thanks the Committee for the opportunity to provide this submission. Should further information be required, the AFP would be happy to discuss further at our appearance before the Committee on 7 August 2020.

Statistics on AFP use of TOLA powers

5. The AFP's use of TOLA powers, specifically the number of Technical Assistance Requests (TARs), Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) under the industry assistance framework, is reported annually in line with the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and Part 15 of the *Telecommunications Act 1997*.

6. Likewise, the AFP's use of Computer Access Warrants (CAWs) is reported annually in line with the *Surveillance Devices Act 2004* (SD Act).

2018-2019: AFP use of TOLA

7. The below statistics were published in the 2018-2019 Annual Reports for the TIA Act and SD Act.

Industry Assistance

8. Between December 2018 and 30 June 2019, the AFP issued **five (5) TARs**. These related to investigations into cybercrime, drug importation and the threat of transnational serious and organised crime.

9. No TANs or TCNs were issued by the AFP, and no State or Territory police forces sought the AFP Commissioner's approval to issue TANs under the industry assistance framework.

10. The AFP has good relationships with domestic communication providers and we are committed to proactively engaging them – recognising industry's advice, expertise and knowledge is invaluable to our work. Our experience is that Schedule 1 of TOLA has accelerated cooperation from industry, with providers increasingly willing to assist due to TOLA providing legal certainties and assurances regarding the commercial scope and impact of requests.

11. The fact the AFP has not sought any TANs or TCNs to date, does not indicate these provisions are not required. Rather, it demonstrates the effectiveness of TOLA's tiered approach.

Computer Access Warrants

12. Between December 2018 and 30 June 2019, the AFP obtained **seven (7) CAWs**, two of which were extended. An additional one (1) CAW application was refused by the issuing authority, due to concerns that a physical computer had to be identified.

2019-2020: AFP use of TOLA

13. The below statistics are those which will be provided to the Minister for Home Affairs under our annual reporting obligations. We provide them here to ensure the Committee has the most recent available figures, to facilitate your oversight and review of TOLA.

Industry Assistance

14. Between 1 July 2019 and 30 June 2020, the AFP issued **three (3) TARs**, which related to serious computer offences and other serious crime types.

15. The AFP did not issue any TANs or TCNs, and no State or Territory police forces sought the AFP Commissioner's approval to issue TANs under the industry assistance framework.

16. As set out above at paragraphs 9-11, TOLA has facilitated successful engagement with industry without needing to compel their assistance.

Computer Access Warrants

17. Between 1 July 2019 and 30 June 2020, the AFP obtained **sixteen (16) CAWs**.

18. In addition to the refused application in 2018-2019, a further two applications in the same matter were also refused. However, the warrant was ultimately issued during the 2019-2020 reporting period.

Operational case examples

19. The below case examples demonstrate the benefits of the TOLA powers.

20. Should the Committee require further technical or operational detail, the AFP can provide this by way of a closed hearing or confidential submission.

Cybercrime – Remote Access Trojan malware *(before court)*

This matter involved an investigation into the possession and use of "Imminent Monitor – Remote Access Trojan" (IM-RAT) malicious software (malware). The malware allowed remote and secret control over a victim's computer and other devices, to access and view files, record keystrokes and activate the computer's web camera.

A statistically high percentage of Australian-based purchasers of IM-RAT (14.2%) are named as respondents on domestic violence orders, and one of the purchasers is also registered on the Child Sex Offender Register.

Without these powers, the AFP would have been unable to proactively investigate and capture relevant data and evidence stored in Australian and other participating countries, or identify victims and prosecute users of this malware. The TOLA powers also enabled the AFP, and our partners, to identify and stop other serious crimes, including computer misuse, fraud, dealings in the proceeds of crime, narcotics and sexual offences.

An overt search warrant would have alerted the criminals using this malware, precluding further identification, disruption and prosecution on ancillary offending being facilitated by the malware. A traditional search warrant would only yield a limited subset of the customer database (noting the purchase may be made in cryptocurrency and untraceable), and this would not have assisted proactive or the targeting of investigations on the users of the malware.

Outcomes

As at 30 November 2019 in relation to this investigation:

- 85 warrants had been executed internationally
- 434 devices have been seized (laptops, phones and servers etc.)
- 13 people have been arrested (none yet in Australia)
- The website selling the malware has been taken down.

Cybercrime DDOS attack on government infrastructure *(before court)*

The AFP used TOLA powers during an eight-month investigation into the use of a carriage service to make threats, identify data sets of compromised personal information, inform Australian government and public telecommunications infrastructure of cyber vulnerabilities and compromise and prevent online fraud. This was a parallel investigation to a State police operation investigating dedicated denial of service attacks against their own telephone infrastructure.

TOLA powers were of significant benefit in this investigation, as they enabled the AFP to obtain evidence from multiple electronic systems used by the alleged offender to commit a variety of offences. Information obtained using TOLA powers also identified further avenues of police enquiry, filled significant evidentiary gaps in relation to the alleged offending, and better-directed police resources in relation to this investigation. A significant proportion of material obtained using TOLA powers is relied on in a brief of evidence in relation to the accused.

Outcomes

Two men were charged on 14 June 2019 with offences including:

- Unauthorised access to data held on a computer;
- Using a carriage service to make a threat or cause serious harm;
- Dishonestly obtaining or dealing with personal financial information;
- Sabotage; and
- Firearm offences.

Importation of illegal drugs

The AFP used enhanced search warrant provisions, to execute a section 3E search warrant on a premises, following the suspected importation of illegal drugs which were procured with cryptocurrency via a dark web marketplace.

During execution of the search warrant, the accused was served a notice to assist in accordance with the updated section 3LA provisions. Following consideration of the order and being advised of the new penalties (up to 10 years imprisonment), the accused provided the AFP with passwords to a number of devices, as well as a number of cloud-hosted accounts through which he had facilitated the importation.

This demonstrates the utility of increased section 3LA penalties. Through the provision of this assistance, the AFP was able to successfully access, identify and collect otherwise secure and encrypted communications and digital records as evidence of the alleged offending.