AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION

OFFICIAL

Australian Criminal Intelligence Commission submission to the review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

The Australian Criminal Intelligence Commission (ACIC) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's (the Committee) review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (the Bill).

Criminal threat environment

The operating environment for Australia's law enforcement and intelligence agencies has become increasingly challenging due to criminal uptake of new technologies and methodologies. Criminals are increasingly using the Dark Web and dedicated encrypted communication platforms to facilitate and undertake a wide range of serious crimes, including money laundering, illicit drug and firearms smuggling, and the production and dissemination of child exploitation material. The encryption and anonymisation that underpins the Dark Web and encrypted communications has challenged existing powers and allowed serious and organised crime (SOC) groups and individuals to more effectively conceal their criminal activity. In particular, the networks established on the Dark Web and via encrypted communications have provided criminals with platforms to easily and more confidently communicate anonymously about, and obfuscate, their serious criminal activities.

The electronic surveillance powers currently available to the ACIC, while relied upon for investigating many aspects of criminal behaviour online and criminal use of encrypted communications, are not sophisticated enough to identify and disrupt the totality of activities SOC entities are undertaking through the use of modern anonymising technologies to conceal their identities, their associate's identities and the illegal activities being undertaken by the network of individuals.

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) was enacted as one legislative response to address challenges that technologies like encryption pose. While the powers introduced by the TOLA Act have significantly assisted the ACIC's effort to tackle online criminal threats cloaked by advanced encryption and anonymising technologies, more is needed to provide the ACIC and AFP with effective powers to combat the rising tide of cyber-enabled crime. No single legislative amendment can wholly address the increasing challenge posed to agencies in determining who serious offenders are and what they are planning. A variety of powers are necessary to ensure that the ACIC and AFP are enabled to keep Australians safe.

The ACIC's powers must maintain pace with emerging threats

The ACIC seeks the amendments sought under this bill in order to fulfil its role as Australia's national criminal intelligence agency, through the collection, assessment and dissemination of criminal intelligence and information, in order to inform national strategies to address transnational serious and organised crime.

To deliver on this purpose, the powers and capabilities of the ACIC must keep pace with technological trends and emerging threats to ensure the agency is able to adequately tackle serious cyber-enabled crime and sophisticated criminal groups using encrypted platforms. With a vast depth of operational expertise and access to the latest technical and analytical tools, the agency must be enabled to support law enforcement outcomes to protect Australians against the most sophisticated and high-threat actors, who increasingly utilise advanced communications technologies to mask their criminal activities. Enhancing the ACIC's ability to collect intelligence, investigate and disrupt criminal activity should be a priority to ensure its enduring ability to respond to the challenges posed by criminals impacting Australia.

The central purpose of the Bill is to provide the ACIC and AFP with the powers needed to continue enforcing the criminal law and protecting the Australian community. The Bill's disruption, intelligence collection and account takeover powers will complement the ACIC's existing powers by providing new avenues to gather information and respond to serious crime occurring online and criminals using dedicated encrypted communication platforms. The measures in the Bill are grounded in the principle that the powers granted by Parliament to the agencies charged with enforcing the criminal law should not be eroded by advances in technology. The Bill is designed to provide the ACIC and AFP with the ability to protect the Australian community from harms online in the same way they protect Australians in the physical world.

New Powers

The Bill addresses gaps in current electronic surveillance powers to enable the ACIC to discover, target, investigate and disrupt the most serious of crimes, including drug trafficking, illicit firearms trade and money laundering. The Bill is one part of the Australian Government's response to counter criminal activity online, including on the dark web, as highlighted in Australia's Cyber Security Strategy 2020. The Bill supports the objectives of the Strategy by establishing a robust and durable framework for law enforcement to respond to the challenges posed by anonymising technologies, encryption and cyber-enabled crime.

While the TOLA Act greatly assisted law enforcement to combat SOC groups at the time it was enacted, further advancements in agencies' powers are required to meet technology developments. Criminal use of the Dark Web and anonymising technologies is a prime example of how powers available to Australian law enforcement must be updated to keep pace with developments in technology.

Encryption and anonymising technologies have a valuable role in protecting the privacy and data of Australians. As such, the ACIC notes new powers cannot be exclusively focused on subverting encryption and anonymising technologies. Instead new powers must provide the ability for agencies, like the ACIC and AFP, to access material at unencrypted points, or to utilise their capabilities to see through the obfuscation that nefarious use of these technologies provide.

The ACIC will use the new powers outlined in the Bill to focus efforts on understanding and gathering intelligence on TSOC groups who are using encrypted communication platforms to conceal their criminal activities . These platforms are used almost exclusively by SOC groups and are developed specifically to obscure the identities of the involved criminal entities and enable avoidance of detection by law enforcement. They enable the user to communicate within closed networks to facilitate highly sophisticated criminal activity. ACIC observation shows there is no legitimate reason for a law-abiding member of the community to own or use an encrypted communication platform.

Network Activity Warrants

Network activity warrants provided by this Bill will immediately transform the ACIC's ability to discover and understand serious criminal groups using the Dark Web and encrypted communication platforms to undertake and facilitate serious crimes. Improving the ACIC's ability to discover and understand SOC entities using this technology will critically enhance the ability of the ACIC to more accurately inform the national understanding of SOC.

Currently, while the ACIC might be able to detect criminal behaviour on a hidden website or computer network, we cannot identify all the individuals participating in the criminal behaviour. For this reason, we require the ability to target and infiltrate the network, or class of computers, in which the crime is occurring so the members of the criminal group can be identified and the full nature and extent of the criminality can be detected through the collection of intelligence. The Bill will amend the *Surveillance Devices Act 2004* to allow the ACIC and AFP to use existing computer access techniques to collect intelligence on the criminal networks most significantly impacting Australia.

Network Activity Warrants – an avenue to understand criminal networks

In the course of an investigation into the trafficking of illicit drugs, the ACIC identifies a type of encrypted handset being sold specifically to TSOC entities to facilitate drug importations. The only known use of this handset is to communicate with other members of drug smuggling syndicates. The device contains only a specialised encrypted communications platform, advertised as being particularly robust against law enforcement intervention. The technology in use poses challenges to law enforcement as all communications are encrypted and the users are anonymised.

A network activity warrant could then be applied for, based on the characteristics that the encrypted platform presents within a service, to collect intelligence on the criminal network planning the drug importation and the wider group of users of the particular specialised handset.

During the course of the network activity warrant, the ACIC would be lawfully enabled to collect intelligence to inform a number of things, including an understanding of the SOC group's members, where they are located and their level of engagement in the criminal enterprise. Further, this intelligence discovery phase may allow for the identification of professional facilitators, such as accountants, who may be assisting the syndicate to conceal proceeds of crime derived from their illicit trafficking activities.

The intelligence gained under this warrant would inform future prevention and disruption strategies, as well as the application for other lawful authorities to effectively target identified individuals at high levels of the criminal enterprise.

Data Disruption Warrants

The transnational nature of SOC, which is increasingly facilitated via anonymous, encrypted online networks, means that offenders often remain anonymous and outside the jurisdiction of Australian law enforcement. For these reasons, disruptions that are short of, or in addition to, prosecution are sometimes the most practical way to combat criminal groups and prevent them from harming Australians. In the physical domain Australian agencies can already lawfully disrupt serious criminal activity by doing things like interdicting drug shipments, freezing assets, confiscating the proceeds of crime, or restricting travel. However, what can currently be done in a digital environment to disrupt serious criminals is comparatively limited.

Data disruption warrants will enable the ACIC to interfere with the data held on online criminal networks or devices, in order to frustrate the commissioning of serious criminal offences. This will be particularly powerful in the context of disrupting criminal activity which is largely occurring online, such as the distribution of child exploitation material, as it will allow the AFP/ACIC to halt the distribution immediately (when observed) through the use of the warrant, or block payments before, rather than after the collection of evidence which, by its nature would not be an immediate activity and would likely allow additional offending to occur.

Disrupting a service to prevent continued access and SOC offending

Through human source intelligence, the ACIC identifies an encrypted communications platform being used by a known criminal syndicate to facilitate SOC, including the importation of commercial quantities of illicit drugs and laundering proceeds of crime. Due to the use of anonymising technologies, the ACIC is unable to identify and locate users to effectively undertake traditional investigative and prosecutorial disruptive action.

On the basis that SOC activity is occurring through use of these platforms, from intelligence gathered through a Network Access Warrant, the ACIC applies for and obtains a data disruption warrant. Once the warrant is issued, the ACIC would be able to remotely access the platform and perform data disruption activities by disrupting communications to and from the platform, making it difficult for offenders to continue using the encrypted handsets and the platform. This may include, for example, changing passwords to prevent users' access to the platform, introducing malware onto the devices connecting to the platform and denial of service attacks to prevent the server hosting the platform from operating. The ACIC may also carry out disruption by removing details of where to deposit money for those seeking to buy the drugs or re-directing the funds transfer into a different financial account without causing a person to suffer a permanent loss of money.

The disruption activities authorised by the data disruption warrant will allow the ACIC to frustrate the criminal activities of SOC entities, while also enabling evidence to be obtained of the service and its users. Information gathered by virtue of disruption may be used in

prosecution of offenders or to support the furthering of the investigation under a subsequent evidence gathering power.

Account Takeover Warrants

Account takeover warrants will allow the ACIC and the AFP to use the trusted relationships and networks that have been built between criminal associates against those same criminals. In many cases, taking control of an online account in conjunction with other investigatory powers will be an efficient method for agencies to infiltrate online criminal networks. This will play a crucial role in uncovering the identities of otherwise anonymous criminals, as well as gathering evidence of the initiation and commissioning of serious offences online, including on the Dark Web and where encrypted communication platforms are in use.

This style of warrant will allow for the disruption of serious offences online by giving the ACIC and the AFP the ability to take control of a suspect's online account or persona for a limited period. Once in control of a target's account we would be able to disrupt crime by preventing access to the criminal network or otherwise adopting a suspect's online persona for the purposes of further understanding a criminal network, influencing that network to support law enforcement operations, and collecting evidence.

Account Takeover Warrants to support investigations into sophisticated TSOC groups

During the course of an investigation into a major TSOC group facilitating the importation and distribution of illicit drugs and proceeds of crime, the ACIC applies for an account takeover warrant. The warrant could provide an avenue to secure evidence against a drug distribution network.

An account takeover warrant, in conjunction with additional authorities, such as a controlled operation authority or computer access warrant, would allow the ACIC to take over an individual's account and to continue communicating with other individuals within the criminal entity, as well as those involved in the organisation of major importations.

Account takeover warrants are critical in this respect as they would enable the ACIC to exploit existing relationships within these criminal networks by enabling ACIC officers (in conjunction with other powers) to assume the persona of these individuals via their accounts. This is more effective as it does not require the agencies to have to attempt to infiltrate the networks and develop new relationships.

Further, in this scenario it is likely high-end encrypted communication platforms would be used by the syndicate. Account takeover warrants would be particularly useful in preserving evidence where the technology itself enables the quick destruction of material on the device which, but for having account takeover powers, the ACIC could not access.

This power would allow the agency to gather further information relating to the networks and their criminal activities to feed into investigations, disruption and prosecution strategies.

ACIC internal processes for warrant applications

Some submissions have raised the concern that any ACIC member can apply for a data disruption or account takeover warrant. The ACIC does not agree this would lead to an inexperienced officer applying for, and executing, a data disruption or account takeover warrant without the appropriate training and oversight mechanisms in place.

As with existing warrants in the *Surveillance Devices Act 2004* (SD Act), data disruption warrants and account takeover warrants can be applied for by law enforcement officers of the AFP and the ACIC. The definition of *law enforcement officer* in existing section 6A of the SD Act includes all employees of, and secondees to, the AFP and the ACIC. The ACIC notes this definition accurately and appropriately covers the ACIC operational workforce.

The ACIC has internal policies and procedures in place governing the application process for warrants. Within the ACIC, warrants are applied for by the principal law enforcement officer for a given operation, following discussion and approval by the relevant team leaders and the relevant state investigations manager. The principal law enforcement officer for an investigation/operation is the person who is most accurately able to depose the affidavit attesting to the existence of particular suspicions which form the basis for the application.

ACIC internal training for warrant applicants and authorising officers

The ACIC strives to achieve the highest standard of compliance with all aspects of reporting, accountability and oversight associated with the SD Act, *Telecommunications (Interception and Access) Act 1979* (TIA Act) and any legislation providing the ACIC with similar intrusive powers.

To achieve this high standard of compliance the ACIC has its Excellence in Compliance (EiC) strategy and training. The EiC has mandatory annual training and assessment requirements for members of staff (including legal officers) who:

- will be applicants for warrants pursuant to the SD Act or the TIA Act; and
- need to access information captured by a surveillance device or a telecommunications intercept or authorisation.

The above compliance controls limit who can access Protected Information, Lawfully Intercepted Information, Lawfully Accessed Information, telecommunication data or the ACIC's interception platform.

Conclusion

As outlined above, it is critical that the ACIC and AFP are provided with new powers to combat cyber-enabled transnational serious and organised crime. This advance in powers is necessary to stay at the forefront in the fight against criminal activity on the Dark Web and those seeking to use encryption and anonymising technologies to hide their criminal activities in the physical world.

The ACIC would welcome the opportunity to brief the Committee further on these matters in a classified setting if it would be of assistance.