



9 March 2022

Electronic Surveillance Reform Taskforce
Department of Home Affairs

Via email: electronicsurveillance reforms@homeaffairs.gov.au

Dear Sir / Madam

Reform of Australia’s electronic surveillance framework – AFP perspectives

Since the AFP’s formation in 1979, evidence lawfully collected from the use of surveillance devices and telephone intercepts has been integral to the success of countless investigations, and critical to the AFP’s mission of Policing for a Safer Australia. The digital age and associated developments in communications technology have however led to significant changes to the AFP’s contemporary operating environment since this time.

It is the AFP’s operational experience that criminals are often early adopters of technological advancements that support secure communications, allowing them to evade law enforcement detection and further their criminal enterprises. We continue to see wide-spread adoption of secure technologies including encrypted over-the-top applications and custom platforms, as well as darknet and anonymising technologies (such as virtual private networks).

While the AFP supports personal privacy and the need for information security, technologies are increasingly being exploited by criminals to avoid lawful detection and access by the AFP and other law enforcement partners. This is occurring across all crime types, including terrorism, child exploitation, and transnational serious and organised crime. For example, of the internet data lawfully intercepted by the AFP in the 2020-21 financial year, 92.3% was unintelligible due to the use of encryption. This highlights the challenges to evidence collection and investigation into criminal conduct that evolving technologies pose.

On 8 June 2021, the AFP publicly revealed Operation Ironside – a long-term, covert investigation into serious organised crime groups responsible for large-scale drug importations and manufacture, attempts to kill and other significant harm to the Australian community. As part of the Operation, the AFP and FBI monitored criminals’ encrypted communications over a dedicated encrypted platform called ‘ANØM’. Users would brazenly discuss their criminal activity, placing their trust in the platform’s security and their belief that law enforcement were unable to monitor their encrypted communications or attribute them to individuals.

The Operation represents a historic blow against serious criminal organisations. As at 13 January 2022, the Australian resolution has resulted in:

- 727 search warrants executed
- 350 offenders charged
- 2261 charges laid
- 141 weapons/ firearms seized
- \$53.7 million seized
- 6,314kg of drugs seized by Australian agencies

The success of Operation Ironside was due to the combined use of legislative frameworks and the cooperation of foreign law enforcement. The outcomes achieved would not have been possible without the electronic surveillance powers vested in the AFP, which are governed by various pieces of legislation.

In recent years the AFP has been granted additional powers to address criminal adoption of technology, such as those contained in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and the recently passed *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*. These Acts support historic powers imparted by the *Telecommunications (Interception and Access) Act 1979* (TIA Act), *Surveillance Devices Act 2004* (SD Act), and parts of the *Telecommunications Act 1997* (Telco Act).

Together, these Acts contain more than 20 different law enforcement warrants and authorisations with varying thresholds and tests for electronic surveillance powers. They create a complex framework, with many of the historic provisions becoming inconsistent, outdated and inflexible in practice with the passage of time. This frustrates the framework's application to modern criminality.

Creation of a new framework

The AFP engaged extensively with Mr Dennis Richardson AO and his team to inform the Comprehensive Review of the Legal Framework of the National Intelligence Community (Comprehensive Review), providing submissions, appearing at public and private hearings and answering questions on notice.

The AFP supports the Comprehensive Review recommendations and Government Response, noting that implementation of these recommendations will have a significant and direct impact on the operations of the AFP, with wide scale legislative reform to consolidate core policing powers in the TIA and SD Acts.

The AFP is not seeking new or additional powers through these reforms. The harmonisation and consolidation of functionally equivalent powers under the proposed electronic surveillance reforms will be crucial for meeting the continuing technical challenge of investigating serious crimes undertaken with the aid of technology.

This will help us to effectively investigate serious crime, while retaining appropriate safeguards and oversights. It is pivotal that the new framework:

- modernise and harmonise existing powers to address evolving criminality,
- be tech neutral, future proofed, to avoid becoming outdated as technology develops and overcome the consequences of the existing patchwork of amendments,
- ensure the current powers (relied on daily) are not lost or further complicated,

OFFICIAL

- be practical, simple and straightforward – this is imperative in order to provide reassurance to community and industry,
- provide reassurance to the community through streamlined and efficient oversight and transparency, and
- place the AFP and our partners ahead of the criminal environment.

These key criteria will ensure the AFP and partner agencies are well placed to address criminality now, and into the future. The AFP will continue working closely with the Department of Home Affairs to ensure this shared goal is accomplished.

Yours sincerely



Ian McCartney APM
Deputy Commissioner Investigations