Australian Government
Australian Commission for Law Enforcement Integrity

Reform of Australia's electronic surveillance framework – Discussion Paper

Submission by the Australian Commission for Law Enforcement Integrity

Contents

Introduction

The office of the Integrity Commissioner, and ACLEI, are established by the *Law Enforcement Integrity Commissioner Act 2006* (Cth) (LEIC Act) to investigate and prevent corrupt conduct in Commonwealth law enforcement agencies.

ACLEI's strategic purpose is to make it more difficult for corruption in law enforcement agencies to occur or remain undetected. We undertake our oversight of law enforcement agencies in four main ways:

- We receive and assess notifications of alleged corrupt conduct by members of Commonwealth law enforcement agencies
- We conduct investigations into serious and systemic corrupt conduct
- We support our partner law enforcement agencies to detect corrupt conduct and perform their own investigations and
- We prevent corruption through training, support and identification of vulnerabilities.

Under the LEIC Act, the Integrity Commissioner has jurisdiction to investigate allegations of corrupt conduct by staff members of law enforcement agencies under her jurisdiction—presently the:

- Australian Criminal Intelligence Commission (including the former Australian Crime Commission, the former National Crime Authority and the former CrimTrac Agency)
- Australian Federal Police (including ACT Policing)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Department of Home Affairs (including the Australian Border Force)
- Prescribed aspects of the Department of Agriculture, Water and the Environment (DAWE)
- Australian Competition and Consumer Commission (ACCC)
- Australian Prudential Regulation Authority (APRA)
- Australian Securities and Investment Commission (ASIC); and
- Australian Taxation Office (ATO);
- Office of the Special Investigator

The LEIC Act requires the Integrity Commissioner to prioritise the investigation of serious and systemic corruption. For this purpose, the Integrity Commissioner has coercive information-gathering powers and a full suite of law enforcement powers including:

- Search warrants
- Controlled operations
- Telecommunications data authorisations
- Telecommunications interception warrants
- Stored communications warrants
- Surveillance device warrants; and

- The power of arrest.

Australia's electronic surveillance framework

The Reform of Australia's electronic surveillance framework – Discussion Paper (the Discussion Paper) sets out a number of issues identified by the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (the Comprehensive Review) in relation to the current framework for electronic surveillance in Australia, including that the current laws are "complex, inconsistent, outdated and inflexible"[1].

As a small law enforcement and oversight agency, ACLEI's experience of Australia's electronic surveillance framework aligns with some of the issues identified by the Comprehensive Review. The different legislative regimes that make up the electronic surveillance framework are complex and inconsistent. They are based on specific technology at a point in time and, as a result, have relied on technological concepts that have dated and created inflexibility.

The most obvious example of this is the regime for telecommunications interception, provided for in the *Telecommunications (Interception and Access) Act 1979*, which is predicated on the interception of communications as they cross over a carriage service. While telecommunication interception continues to be an important law enforcement tool to capture live conversations using carriage services, such as fix line telephones or mobile phones, the limitation of such a technology specific regime has been made evident by the rapid development of technology to include forms of communication such as email and SMS, which might not be crossing over a carriage service when they are intercepted. As a result, new warrant and authorisation regimes have been established to fill the gap, including the stored communications and telecommunication data regimes.

The number of different legislative provisions to covertly access electronic information has created an unnecessary complexity. ACLEI supports this current consideration of the framework as a whole, to ensure that Australia's electronic surveillance regime remains fit for purpose, provides adequate protections in relation to privacy and the information covertly obtained and robust oversight.

While ACLEI supports the consideration of reform in this area, we also note that the current provisions provide access to vital information and evidence in support of our investigations. We foresee that access to information and evidence of this type will have ongoing relevance to our investigations into the future. Our experience is not that the current provisions are unworkable or unnecessary, rather that they are overly complex and inconsistent.

[1] Discussion Paper, page 3

The proposed future state for Australia's electronic surveillance framework

A technology neutral framework

The Discussion Paper sets out a number of principles to consider in relation to a future state for Australia's electronic surveillance framework. It does not attempt to draft these principles into legislation, given the early stage of this consultation. The clear lesson from the current electronic surveillance regime is that a future state should be technology neutral, given the rapid changes that occur in relation to communication technology. However, while the principle is clear, the drafting of legislation to ensure technology neutrality is likely to be complex, with input from a range of specialists required to ensure that the provisions operate as intended and provide law enforcement with, at the very least, access to the same information that can be accessed under the current provisions.

In addition to complexity in the drafting process, legislative provisions that relate to electronic surveillance can, by their nature, be complex. An example of this can be seen at page 25 of the Discussion Paper in relation to the definition of 'content' in the *Investigatory Powers Act 2016 (UK)*. For a future state electronic surveillance framework to meet the guiding principle of being "clear, transparent and useable for operational agencies and oversight bodies, as well as industry who need to comply with the obligations of the framework"[2], the drafting of the provisions must be clear and unambiguous, without any unnecessary complexity.

An outcomes based framework

The Discussion Paper raises a future state warrant framework based on outcomes (i.e. types of information) rather than methods of access. Such a framework might allow an issuing officer to issue a warrant to capture types of information without limiting the method used[3].

As electronic surveillance warrants authorise conduct that would otherwise be a criminal offence, a warrant that did not limit the method used to engage in that conduct would need to be carefully and clearly drafted to ensure that law enforcement officials did not inadvertently engage in criminal activity.

Consideration of the least intrusive method

The Discussion Paper also indicates that under the new framework, the law enforcement agency will likely be required to satisfy the authorising officer that the proposed method for access is the least intrusive method available, while still being effective.[4] It is not clear how a framework based on outcomes rather than methods aligns with a framework where the method is a key consideration. Regardless of this, the inclusion of a requirement to authorise the least intrusive method available is sensible if there are multiple methods that could be used to obtain the information.

---

[2] Discussion Paper, p 6.

[3] Ibid, p.34.

[4] Ibid, p.35.

Such a requirement would need to be balanced with the effectiveness and timeliness of the proposed method. For example, if a less intrusive method of obtaining the information takes more time and this additional time creates the potential for the information to be destroyed prior to access under the warrant, it might not be preferred to a more intrusive method of obtaining the information.

Harmonisation of legislative thresholds

In response to the principle found by the Comprehensive Review that powers that are functionally equivalent should have the same limits, controls and safeguards, the Discussion Paper indicates that a new framework would seek to harmonise legislative thresholds for functional equivalent powers[5].

The legislative thresholds for the current electronic surveillance powers are different and have grown more complex with the addition of further offences as exceptions to general thresholds. For example, the definition of "serious offence", which is the legislative threshold for a telecommunication interception warrant, is now a complex definition which is over 7 pages long, containing both general types of offences and specific offences.

Harmonising the legislative thresholds and streamlining that threshold will simplify the regime. The Discussion Paper suggests a threshold for law enforcement which is based on having a reasonable suspicion that a person has or is likely to commit an offence with a penalty of at least 5 years imprisonment. This threshold would cover the offences that are typically investigated by ACLEI, such as:

- Bribery of a Commonwealth public official – s141.1 of the Criminal Code (10 years imprisonment)
- Corruption benefits given to, or received by, a Commonwealth public official – s142.2 of the Criminal Code (5 years imprisonment)
- Abuse of office – s142.2 of the Criminal Code (5 years imprisonment).

It is important to note, however, that harmonisation of legislative thresholds should apply where the powers are functionally equivalent. As the Discussion Paper sets out in Part 2, information about a communication and the content of a communication are different. Powers that enable access to information about the communication should be considered as being different to powers that enable access to the communication and can appropriately have different legislative thresholds. Similarly, the Discussion Paper raises the difference between tracking information as opposed to other surveillance information, which provides more detailed information about a person's conduct, which might also be appropriately dealt with through different legislative thresholds.

In the same vein, legislative provisions relating to periods for data retention should also be harmonised so that requirements to destroy data do not create obstacles to access such data for the purposes of criminal investigations or—in the case of ACLEI—investigations under the LEIC Act.

Target based warrants

Given the intrusive and covert nature of electronic surveillance, it is appropriate that electronic surveillance is directed at the person of interest. In the example of law enforcement, this means being directed at the person suspected of having committed or likely to commit an offence.

[5] Ibid, p 39.

There will be exceptions where electronic surveillance will need to be directed at a particular device or a third party, as is currently provided for. These exceptions can include additional tests, as is currently the case, to ensure that they are used appropriately. The Discussion Paper provides an example of an additional test for third party warrants, that obtaining the information directly from the person of interest would be impractical or inefficient. This is similar to the additional considerations that a Judge or AAT member must currently have regard to in issuing a third party telecommunications interception warrant (known as a "B" party warrant). These additional considerations in section 46A of the *Telecommunications (Interception and Access) Act 1979* are:

> (2) For the purposes of subsection (1), the matters to which the Judge or nominated AAT member must have regard are:
>
> (d) the what extent methods (including the use of a warrant issues under section 46) of investigating the offence or offences that do not involve the use of a warrant issued under this section in relation to the person have been used by, or are available to, the agency; and
>
> (e) how much the use of such methods would be likely to assist in connection with the investigation by the agency of the offence or offences; and
>
> (f) how much the use of such method would be likely to prejudice the investigation by the agency of the offence or offences, whether because of delay or for any other reason.

Necessary and proportionate tests

The Discussion Paper notes that while there are tests within the current electronic warrant regime that go to impact on privacy, gravity of the offence and availability of other investigative methods to obtain the information, there is currently no explicit necessary and proportionate tests[6].

Given the intrusive nature of electronic surveillance and the privacy impact of the collection of this information, it is appropriate that these powers are only used when they are necessary and that their use is proportionate to the gravity of the matter under investigation. While these are matters that should be implicitly considered when applying for a warrant under the current regime, ACLEI supports these being explicitly referenced as considerations in the future state electronic surveillance regime.

Disclosure of information obtained under a warrant

ACLEI's experience is that it is often necessary to disclose information obtained under an electronic surveillance warrant for reasons including:

- For the purposes of prosecution
- To other law enforcement agencies in relation to joint investigations
- For oversight by the Commonwealth Ombudsman.

ACLEI supports a principles based and tiered approach to use and disclosure of information obtained under a warrant. We also note that disclosure provisions should be drafted as clearly as possible, given that they will amount to exceptions to offences for unauthorised disclosure.

[6] Ibid, p 51.

Oversight of the electronic surveillance regime

A strong oversight framework for electronic surveillance is vital to ensuring ongoing confidence in the regime, given the intrusive and covert nature of electronic surveillance. For Commonwealth law enforcement agencies, this oversight is currently performed at different times by:

- the issuing authority, in considering whether the conditions to issue the warrant has been met
- the courts, in considering the admissibility of evidence obtained through the warrant; and
- the Commonwealth Ombudsman, in inspecting the use of the powers by agencies.

ACLEI supports this ongoing oversight being continued into the future state electronic surveillance regime and enhanced where necessary.