Submission No 209

Inquiry into potential reforms of National Security Legislation

Organisation: ASIO

National Security Legislation Reform

The Parliamentary Joint Committee on Intelligence and Security has been asked to examine a package of national security ideas comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform. The terms of reference and a discussion paper which provide explanation of the reform proposals have been published on the Committee's website.

The reform proposals are about properly equipping our law enforcement, security and intelligence professionals to do the job that Australians have entrusted to them. They are also about continuing to ensure that the Australian telecommunications sector is properly protected.

In this document ASIO discusses data retention and why this is considered necessary in the context of the *Telecommunications (Interception and Access) Act* 1979 (the TIA Act) and the security intelligence functions of ASIO.

Modernisation of the Telecommunications (Interception and Access) Act

What do we use Telecommunications Interception (TI) for?

TI is a critical operational tool for security, law enforcement and integrity agencies. It cannot easily, or without considerable cost or risk, be substituted with any combination of alternative investigative techniques.

For ASIO and law enforcement agencies, TI provides a unique, low risk and cost effective tool for collecting intelligence and evidence. It can only be used in very specific circumstances. For ASIO, this threshold is very high. ASIO must be confident that there is a link between the telecommunications activity to be intercepted and activities that are intended to do harm to Australia or its people. Furthermore, ASIO rules dictate that interception can only be carried out after consideration of the proportionality between the nature and seriousness of the threat, the degree of intrusion and the overall impact on privacy. The independent Inspector General of Intelligence and Security routinely inspects ASIO's TI operations to ensure this is the case.

Communications material is vital in two respects:

1. the actual content of telecommunications, telephone conversations, emails and messages which forms the basis for intelligence assessment and investigations and may be used as evidence in court proceedings. The actual content may be collected only on the basis of a warrant.

2. the so called 'meta-data' or 'communications associated data (CAD)' which is essentially information generated alongside the communication and is identifying information about the originator, recipient, location and timing of calls, etc. This data is vital to law enforcement and security intelligence agencies for pre-warrant checks, investigative leads, intelligence and evidentiary corroboration, etc. It may also be used in evidence. Collection of this telecommunications data, as opposed to content, does not require a warrant.

Current TI Regime

All carriers and carriage service providers (C/CSPs) have an obligation under the TIA Act to install and maintain an interception capability within their networks and to make that capability available to authorised interception agencies. That capability may include access both to the actual content of the communication (but only under warrant) and to CAD.

The interception model in Australia is currently based on a service or equipment identifier. These identifiers include telephone numbers, email addresses, or unique numbers attached to telecommunications hardware (e.g. mobile phone handsets, or individual computers, etc). Warrants for interception of content within telecommunications networks can only be issued on the basis of these network identifiers.

Agencies currently intercept on the basis of those network identifiers via the following warrant types:

- *Telecommunications service warrant*
  A telecommunications services warrant enables authorised agencies to intercept communications from a specified telecommunications service (e.g. mobile phone) either because it is being used by a person reasonably suspected of engaging in activities prejudicial to security or the service itself is being used for purposes prejudicial to security.

- *Telecommunications service (B-party) warrant*
  Where the service of the person involved in activities prejudicial to security cannot be identified or intercepted, ASIO may request interception of services belonging to another person known to communicate with the person of interest.

- *Named person warrant*
  Where it is ineffective to rely on a telecommunications service warrant to obtain the requisite intelligence, ASIO may request authority to intercept all telecommunications services that are used by the person of interest.
  There are two categories of this named person warrant – named person (services) and named person (devices). The former authorises interception of all known telecommunications services (for example, home phone, business phone, mobile phone, facsimile, and email) whereas the latter authorises interception of specified devices connected to the person (e.g. multiple mobile phone handsets).

Current protections for access to communications and to data

ASIO is, appropriately, subject to significant oversight and accountability mechanisms. These, combined with specific protections under the current Telecommunications Interception regime provide a high level of assurance to the Australian community that its security intelligence service acts responsibly and with proportionality. These protections include:

- ASIO may only listen to or record (ie intercept) the content of communications passing over the Australian telecommunications network under the authority of a warrant issued by the Attorney-General or where otherwise authorised under the Telecommunications (Interception and Access) Act.

- ASIO may also only access the content of stored communications held on a carrier/carriage service provider's equipment (such as emails, SMS and voice mail messages) under a warrant issued by the Attorney-General.

- The Attorney-General must be satisfied that the request meets the legal tests (for example, whether the telecommunications service to be intercepted is likely being used by a person engaged in activities prejudicial to security) before issuing a warrant.

- ASIO accesses telecommunications-associated data (i.e. not content) from carriers/carriage service providers under internal authorisations which may only be made where the relevant ASIO officer is satisfied that the disclosure of the data specified in the authorisation would be in connection with the performance of ASIO's legal functions (and for no other purpose).

- In all cases, before requesting a warrant or making an authorisation, consideration must have first been given to the requirements of the guidelines issued by the Attorney-General under the ASIO Act which include:

    - inquiries and investigations are to be undertaken using as little intrusion into individual privacy as possible;

    - wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and

    - any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence.

- The Inspector-General of Intelligence and Security routinely undertakes inspections of warrants, warrant related document and authorisations for the disclosure of telecommunications data to ensure that ASIO acts within its legal authority and with propriety and reports on these issues in the Inspector-General's annual report.

- ASIO reports to the Attorney-General within three months of the expiry or revocation of a warrant on the extent to which the interception of communications under the warrant has assisted ASIO in carrying out its functions.

Communication Associated Data (CAD) – data retention

In the context of TI reform "data" or CAD generally refers to *information about communications* – not the actual substance or content of those communications. For example: phone number xxxxxxxxxx called number yyyyyyyy at 10:00 on 12 September 2012; not what was said during the conversation.

For many years law enforcement and security agencies (as well as many others) have been able to request CAD from any carrier or carriage service provider. Agencies access to this information through an internal authorisation. This power already exists; a brand new power is not being sought.

Traditionally the telecommunications industry has retained the call data, and many still do, mainly for billing purposes. However, over time, technological and business changes have meant that industry has less need to retain the sort of CAD information agencies require. The main drivers are the increased use of Internet Protocol (IP) technology and the trend to charge customers based on volume (units of data sent or received) rather than by transaction (ie. call by call, message by message).

This situation is becoming more common around the world and has led many jurisdictions to consider mandatory retention of CAD for law enforcement and security purposes.

CAD is used by agencies to determine who communicated with whom, when, where to and where from. Its use is often the most appropriate and proportionate response to investigative leads. This information assists in refining/focusing an investigation and ensures individuals who are not relevant to the investigation can be ruled out at the earliest possible opportunity.

CAD is often received as important "lead" or "tip off" information. For example it may demonstrate that an Australian telephone number has been in contact with a member of a terrorist cell in a foreign country or that an Australian internet address has been the subject of cyber attack.

CAD may be used to corroborate intelligence or evidence, exclude or include persons in an investigation, or to provide locational information.

CAD data also provides a critically important part of broader security or law enforcement requirements. It can be used to help identify perpetrators or victims of malicious activity on the internet. It can be used to help locate victims of crime or individuals in distress.

To the extent possible, agencies are seeking greater certainty that the information needed to protect the community will be there when they need it. In that sense agencies are looking to access the same general information they have been accessing for many years; information that would enable them to trace the participants of a communication in retrospect, when the communication occurred and ideally where the parties were. It might include:

- data to identify the parties of a communication;
- data to identify the origin and destination of a communication;
- data to identify the date, time and duration of a communication;

- data to identify the type of communication (eg. phone call, email)
- data to identify users' communications equipment; and
- data to identify the location of parties to the communications.

In this context, agencies are not seeking access to the content of communications.

The period that CAD is available to law enforcement and security intelligence agencies has a direct impact on its utility for investigations. Investigations of serious criminal activity and threats to security are often long and complex. The identity of all persons of interest may not initially be known and often additional persons of interest will emerge as investigations unfold. The longer relevant data is available to access, the greater the potential utility for the agencies. Given complex investigations are measured in years rather than months, access to CAD for a minimum period of two years is proposed to ensure that agencies can undertake effective investigations in accordance with their functions. Shorter periods of access carry the risk that agencies may be less able to access the critical intelligence that they require to progress an investigation.

The European Union Data Retention Directive provides a useful outline of the types of data requested and is an important basis for discussion with Australian C/CSPs, agencies and other stakeholders. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML)

To ensure privacy protections remain appropriate it may be necessary to include new penalties for misuse of retained data as well as an appropriate scheme for the notification of data breaches. Agencies would support the introduction of such measures provided that there were appropriate exemptions in place to protect sensitive operational information.

Summary

- Any new regime should maintain the distinction between the interception of content and access to communications data.

- Any new regime should retain the current effective oversight and accountability mechanisms which help ensure interception capabilities are used for appropriate and legal purposes and only by the agencies authorised to conduct such activities in the public interest.

- From the point of view of security and law enforcement agencies retention of CAD information has important investigative advantages.