Interception Regulation up for Review

Shane Barber & Lisa Vanderwal examine current proposals for telecommunications interception reform in light of changing technology and threats.

Australia's current telecommunications interception regime was established in 1979. In this pre-September 11 2001 environment, Australia and the world were simpler places in which to live. Many of the technological developments we take for granted today were simply unimaginable. Security threats too were a little more predictable.

In 2012 we are still served by the same core piece of legislation that served us in 1979, the *Telecommunications* (*Interception & Access*) Act 1979 (Cth) (***TIA***), albeit that it has been the subject of significant incremental change over the years. It is the powers afforded under the TIA which almost daily serve as a frontline tool used by law enforcement agencies in dealing with domestic and international security threats. It is also the TIA which, daily, seeks to balance the competing demands of protecting the rights of individuals to express themselves freely with the right of individuals to live free from the threats of others.

It is the powers afforded under the TIA which almost daily serve as a frontline tool used by law enforcement agencies in dealing with domestic and international security threats

In this article we briefly examine two recent developments in relation to the TIA. One represents yet the latest piece of tinkering with the TIA, in the form of the *Cybercrime Legislation Amendment Bill 2011* (the ***Bill***). The other reflects the opening salvo in a more comprehensive approach to telecommunications interception reform currently under consideration by the Parliamentary Joint Committee on Intelligence and Security (***Parliamentary Joint Committee***), using as the basis for its consideration a July 2012 discussion paper prepared by the Commonwealth Attorney General's Department entitled *Equipping Australia Against Emerging and Evolving Threats* (***Discussion Paper***).

The Current Interception Regime

The TIA currently reflects a well-worn regime pursuant to which law enforcement agencies may require telecommunications carriers and carriage service providers (for the purpose of this paper, referred to as ***carriers***) to intercept and subsequently disclose communications passing over a network in real time, and also seek access to communications that have already passed over the network (known as stored communications).

The overriding principle of the TIA is that the privacy of users of telecommunications services in Australia is paramount, with the expectation being that any access to those communications by law enforcement agencies may only occur in tightly controlled circumstances. Generally, to access content, national security and law enforcement agencies must obtain an independently issued warrant and thereafter remain subject to a range of accountability measures. While exceptions are made in relation to, for instance, an employee of a carrier undertaking activities which are reasonably necessary to be done by that employee in order to perform certain duties effectively, even that exemption remains subject to court oversight.

Since it was assented to in October 1979, the TIA has been subject to no less than 78 pieces of amending legislation, not including the Bill. A key series of changes occurred in 2006 with the introduction of a chapter into the TIA dealing with stored communications. The drafters of the TIA could not have imagined back in 1979 many applications of communications networks taken for granted today which do not involve simple real time voice telephony. It is clear though that even with those significant 2006 changes dealing with evolving non-real time material, the legislation is failing to keep up with communications technology and the ingenuity of its users.

The Parliamentary Enquiry

At the time of writing, the Parliamentary Joint Committee armed with terms of reference detailed in the Discussion Paper, has been conducting a series of meetings with stakeholders with a view to reporting to the Federal Government as to whether an entirely new interception regime, which better reflects the contemporary communications environment, should now be put into place.

The Discussion Paper reflects proposals for a package of changes in relation to national security, many of which go beyond recommendations for changes to the TIA. Other groups of proposals are:

- suggested amendments to the Telecommunications Act 1997 to:
  - establish a risk based regulatory framework to better manage national security challenges to Australia's telecommunications infrastructure;[1] and
- proposed reforms to the Australian Security Intelligence Organisation Act 1979 and the Intelligence Services Act 2001.

Insofar as the reforms directly relate to the TIA, in its terms of reference to the Parliamentary Joint Committee the Commonwealth Government has indicated that it wishes to progress the following proposals:

1. Strengthening the safeguards and privacy protection under the access regime in the TIA. This would include examination of:
   (a) the legislation's privacy protection objective;
   (b) the proportionality tests for issuing warrants;
   (c) mandatory record keeping standards; and
   (d) oversight arrangements by Commonwealth and State Ombudsmen.
2. Reforming lawful access to communications regime. This would include:
   (a) reducing the number of agencies eligible to access communication information;
   (b) the standardisation of warrant tests and thresholds;
   (c) streamlining and reducing complexity in the access regime. This would include:
      (i) simplifying the information sharing provisions that allow agencies to cooperate;
      (ii) removing legislative duplication; and
   (d) modernising the TIA's cost sharing framework to:
      (i) align industry interception assistance with industry regulatory policy; and

1 Equipping Australia Against Emergency and Evolving Threats, Attorney General's Department, July 2012, page. 4.

(ii) clarify the Australian Communications & Media Authority's regulatory enforcement role.

Stakeholders appear to agree that there is significant merit in those proposals.

While the Government has flagged its intention to now progress with those proposals, it has also asked the Parliamentary Joint Committee to consider a number of further measures including:

- creating a single warrant with multiple telecommunications interception powers; and
- expanding the number of telecommunications industry participants, beyond just carriers, to which the regulatory regime will apply.

In relation to the concept of a single category of warrant, industry experts have cautioned that such an approach does not take into account the fact that different thresholds are required for the exercise of different types of powers, which may need to be exercised by law enforcement and security authorities.[2]

> There are a range of difference activities with a range of different levels of intrusiveness … and they're reflected in the various levels of thresholds that apply to the granting of each of those warrants. What we're concerned about … is that in creating a single category of warrant we would be adopting a lowest common denominator approach.

The third item on the Government's wish list in relation to the TIA, and in relation to which it has asked the Parliamentary Joint Committee to report, includes matters such as establishing an offence for failure by industry participants to assist in the encryption of communications, to mandate industry response times and, most controversially, mandating data retention periods of up to two years for certain data. It is this latter proposal regarding data retention periods that has attracted significant attention due to the cost and inconvenience it will cause, the implications of which will ultimately be passed on to customers.

An example of how these reforms, if implemented, may manifest themselves in midsized carriers was provided in the submissions of iiNet to the Parliamentary Joint Committee in September 2012. In speaking to the Committee, iiNet's Chief Regulatory Officer, Steve Dalby, is reported as giving the following example:

> Dalby said that iiNet's total band width of 200Gbps could generate some 5 million URLs per second – data that, under the proposed legislation, the ISP would need to retain securely and reliably for two years. He said this would force the company to invest heavily in services and storage. 'We can currently purchase a 4TB disk for about $2,000 – we would need 10,000 of these to store 20,000TB of data. We'd put 10 of those in a rack so we would need 1000 racks' he said.
>
> Dolby added that iiNet would need to build a data centre to house the IT equipment, which would cost an estimated $30 million … All these costs, Dolby explained, would flow through to iiNet customers at an estimated $5 increase per month for all services.[3]

Similar sentiments are echoed by industry bodies such as Communications Alliance Limited and Australian Mobile Telecommunications Association (AMTA), which put forward a joint submission to the Parliamentary Joint Committee. The Australian Information Industry Association and the Australian Industry Group also endorsed the positions taken by Communications Alliance and AMTA in their submission. In their submission, the AMTA and Communications Alliance are reported to have suggested that the Federal Government has not provided sufficient justification for the proposed implementation of data retention and also cautioned that the policy approach to be adopted should see carriers in fact hold as little information as possible to avoid both loss of consumer privacy and any security threats to that information from unlawful access to the retained data itself.[4]

The overriding principle of the TIA is that the privacy of users of telecommunications services in Australia is paramount, with the expectation being that any access to those communications by law enforcement agencies may only occur in tightly controlled circumstances

In the Discussion Paper, the Government makes its case for pushing this extensive reform by noting that:

- Lawful interception under the existing TIA arrangements is highly effective, taking into account the number of arrests, prosecutions and convictions based on lawfully intercepted material.
- Australia is and will remain a terrorist target for the foreseeable future, with jihadist terrorism being the most immediate threat. The Government cites at least four mass casualty attacks which have been disrupted in Australia in recent years due to the work of intelligence agencies. The Government points to the role of examining intercepted conversations in foiling some of these attacks.
- The rapid adoption of telecommunications technology and high speed broadband internet has expanded significantly the frequency of high tech crime being committed when compared to the environment that existed when the TIA was established in 1979. It argues that individuals involved in these activities are highly sophisticated, using highly effective software, ciphers, and other methodologies to impede detection by law enforcement agencies. Real time interception alone is increasingly underequipped to deal with these emerging threats.
- Duplication and complexity, which has arisen as a result of the large number of amendments made to the TIA over the years, needs to be removed.
- The number of telecommunications industry players has, of course, massively increased from the one significant player in 1979:

  > At the end of June 2011, there were 287 fixed line telephone service providers, three mobile network operators, 176 voice over internet protocol services providers, 33 satellite providers and 97 internet service providers (only including ISPs with at least 1,000 subscribers).[5]

- Australian consumers are increasingly accessing multiple technology and services to communicate, with 26% of adults in June 2011 using at least four communication technologies, being fixed line telephony, mobile phone, VOIP and the internet.[6]

---

2 Security reforms must protect consumers from increased powers, says Gilbert & Tobin, Communications Day, Decisive Publishing, 28 September 2012, page 6.

3 Proposed data retention laws will leave industry $400m poorer over two years: iiNet, Communications Day, Decisive Publishing, 28 September 2012, page 5.

4 Proposed Security Regime: AMTA, Comms Alliance warn against cost hit for telcos, Communications Day, Decisive Publishing, 28 August 2012, page, 1.

5 Equipping Australia Against Emerging and Evolving Threats, Attorney General's Department, July 2012, p. 18.

- Social media use, again non-existent in 1979 and barely existent at the time of the 2006 reforms to the TIA, has dramatically increased in recent years providing another avenue of communication which needs to be readily interceptable.

The Discussion Paper concludes that many of the legacy assumptions that existed in the 1970s simply no longer apply. Those assumptions included:

- communications to be intercepted are easily identified;
- the stream of traffic to be intercepted can be isolated;
- carriers control the traffic passing over their networks;
- intercepted communications are easily interpreted or understood; and
- there are reliable sources of associated communications information that link people with identifiers and identifiers to communications.[7]

the legislation is failing to keep up with communications technology and the ingenuity of its users

The Cybercrime Legislation Amendment Bill 2011

While the overall reform of the telecommunications interception regime will take some time to play out, a number of recent changes are now before the parliament in the form of the Bill and those changes themselves are proving to be controversial.

The changes in the Bill are a further consequence of the increased need for security and reflect the requirement set out in the Council of Europe Convention on Cybercrime (the Convention). Curiously however, at the time of writing Australia has not signed the Convention. Indeed four member states of the Council of Europe have not yet signed the Convention, and an additional eight member states of the Council of Europe have not ratified it. Of the non-member states, only Japan and the United States have ratified the Convention.

There are four main areas of change under the Bill, being the introduction of:

- historic domestic preservation orders;
- ongoing domestic preservation orders;
- foreign preservation orders; and
- foreign law enforcement authorisations.

There are currently no mandated minimum periods for which carriers are required to keep communications information, such as stored communications or call related information (for example, where the call was made, the length of the call and to whom it was made). Depending on the organisation, such communications could be kept by carriers for as little as a couple of hours, or for as long as week. As a result, if an investigation by an enforcement agency into a serious offence is not at a stage where that agency could apply for a stored communications warrant to access information that is stored by the carrier at that particular time, currently it is likely that communications relevant to the investigation may be removed from the carrier's records.

The purpose of the preservation orders introduced by the Bill is to allow enforcement agencies to require carriers to retain communications which may be relevant to an investigation for a serious offence so the enforcement agency may have access to those communications when the investigation has progressed further. This appears to have the effect of creating defacto standard retention periods on all carriers, something which is proving controversial in the considerations of the Parliamentary Joint Committee referred to above.

There are however some restrictions on seeking preservation orders in the Bill which are meant to act as safeguards:

- An enforcement agency must, at the time of obtaining a preservation order, confirm that it intends within a three month period to apply for a stored communications warrant to access the material the subject of the preservation order. The intent is to ensure that enforcement agencies are serious about requiring the information for the purpose of their investigation. However, it should also be considered that investigations may change and the enforcement agency may revise its need for the information at a later date. While there are procedures that relate to the revocation of preservation orders, it still does not relieve the carrier from having to preserve the relevant information in the first place.
- There must be reasonable grounds for suspecting that there are stored communications relevant to the offence being investigated.
- Only one person can be listed on a preservation order, and only one order can be issued in relation to the same person or telecommunications service. However the reference to the same person does not include where the person has a number of pseudonyms.
- The enforcement agency must also address any privacy issues.

A preservation order requires carriers to maintain the integrity of the stored communications during the relevant period. While a carrier can keep the original communication or a copy, carriers must ensure the relevant communications are not edited, deleted or otherwise changed.

Historic Domestic Preservation Orders

A historic domestic preservation order will require the carrier to preserve all stored communications that relate to the person or service specified in the order. The effective period for a domestic preservation order is quite short, being from the time the carrier receives the domestic preservation order until the end of that day. However, it includes all stored communications relating to the preservation order that the carrier still has on its systems.

A preservation order is just that – an order for preservation of the relevant stored communications. A carrier must keep the relevant communications for up to 90 days after the date of the domestic preservation order. If the enforcement agency revokes the order, the carrier may delete the stored communications.

A domestic preservation order can only be given to an authorised representative of the carrier. This is either the Managing Director or secretary of the carrier, or an employee of the carrier authorised in writing by the Managing Director or secretary of the carrier. This is the same process that currently applies for stored communications warrants.

The preservation of the stored communications under a domestic preservation order does not entitle an enforcement agency to access those stored communications. Instead, the enforcement agency must then apply for a separate stored communications warrant (or applicable interception warrant), which is subject to separate criteria. Only once the carrier has received the actual stored communications warrant may the carrier release the preserved information. Indeed, for the carrier to do so without a stored communications warrant would be a breach of its obligations under both the TIA and Part 13 of the *Telecommunications Act 1997* (***Telco Act***).

As a result, once a carrier has received a domestic preservation order it must keep the stored communications it acquired during the relevant period until the first of:

- 90 days after the carrier received the domestic preservation order;

6 Ibid, p. 18.

7 Ibid, p. 20.

The Discussion Paper concludes that many of the legacy assumptions that existed in the 1970s simply no longer apply

- the expiry of a stored communications warrant (or interception warrant) in relation to the preserved material; or
- receipt by the carrier of a notice revoking the domestic preservation order.

Ongoing domestic preservation orders

Enforcement agencies will also be able to issue 'ongoing domestic preservation orders' requiring carriers to preserve any stored communications in relation to a specific person or service, not only on the day that order was issued, but also for the next 29 days.

Foreign preservation orders

The Australia Federal Police (***AFP***) will be able to issue 'foreign preservation orders', which reflect requests from foreign countries to obtain certain stored communications which might relate to contraventions of certain foreign laws. A foreign preservation order requires carriers to preserve stored communications in relation to a particular person or service on the day that the foreign preservation order was issued.

As is the case with domestic preservation orders, a carrier cannot disclose the stored communications the subject of the foreign preservation order until it receives a stored communications warrant in relation to those stored communications. However, carriers must preserve the stored communications the subject of the foreign preservation order for up to 185 days after the date of the foreign preservation order.

Foreign law enforcement authorisations

The AFP may also issue authorisations for the disclosure of telecommunications data (being non-content related information, such as time, place and duration of a call) where there has been a request for such information from a foreign country. The scope of the disclosure will depend on the type of authorisation issued by the AFP. The AFP is likely to be able to issue foreign law enforcement authorisations from mid-November 2012.

While there appears to be agreement that reform of the TIA is well overdue, many challenges face the Government as it seeks to balance privacy concerns, the minimisation of the burden imposed on industry in conducting what is essentially a public service, and ensuring that Australia's law enforcement authorities may make use of a powerful tool to enhance domestic and international security. Industry stakeholders and the Government will now await the recommendations of the Parliamentary Joint Committee as it seeks to balance what appear to be multiple competing concerns.

Shane Barber is a Partner, and Lisa Vanderwal is Special Counsel, in the Sydney office of communications and technology specialist law firm, Truman Hoyle.