Australian Government
Australian Security Intelligence Organisation

ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

January 2015

www.asio.gov.au

ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Table of Contents

Overview of this submission

ASIO welcomes the opportunity to make this submission and assist the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its consideration of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the data retention bill).

ASIO has addressed the particular questions asked by the committee regarding use of communications data in Part 1 of this submission (after definitions and the executive summary). As anticipated by the committee, some of the detail in addressing these questions is operationally sensitive and would prejudice national security so it has been redacted from the public version of this submission.

This submission reflects the views of ASIO only. It is a continuation of ASIO's previous submissions to the committee during its inquiry into potential reforms of Australia's national security legislation and to the current inquiry by the Senate Legal and Constitutional Affairs References Committee into a comprehensive revision of the *Telecommunications (Interception and Access) Act 1979 (TIA Act)*.

This submission is divided into parts as follows:

Overview of this submission

Definitions

Executive Summary

Part 1 – Answers to the committee's questions

Part 2 – The need for legislative modernisation

Part 3 – The value of data retention

Part 4 – Case studies

Part 5 – Accountability and oversight arrangements

Part 6 – Frequently asked questions

ASIO has provided both a classified submission to the committee as well as this unclassified submission for public release. The public submission simply has text redacted from each part so as to avoid any prejudice to Australia's national security, has been lightly edited where needed, and has some additional information in response to some matters raised in the December 2014 committee hearings.

Definitions

Communications content includes the substance of a telephone call, email, or text message, email subject lines and attachments, web browsing content, chat room discussion, the content of social media posts, and webcam transmissions.

Communications data provides the context of communications, but not the content. The data typically falls into two broad categories: information about the communications and transactional information; and information about the users and devices.

Table 1 on page 7 maps these categories to the kinds of information to be retained in the bill and provides examples. The categories are consistent with the definition previously provided by the Attorney-General's Department to the committee during its inquiry into potential national security reforms in 2012.

In addition, communications data requests are split into requests for:

- **Historical** data, for example, records of communications made over a past period or subscriber information. Such requests can only be made of a service provider by an ASIO employee or ASIO affiliate authorised by the Director-General of Security; and
- **Prospective** data that is yet to be generated for specified services or individuals that are the subject of security investigation. These requests require a higher level of approval than for historical data and within ASIO can only be authorised by an ASIO employee or ASIO affiliate who is in a position that is Senior Executive Service Band 2 or higher.
- **IP addresses** are a numerical label assigned to each device on a network for the purpose of uniquely identifying each device on the network and facilitating directed communications between devices on the network. In the case of the Internet, these IP addresses are assigned by the Internet Service Provider to devices connected to the Internet allowing subscribers to communicate on the Internet. In some cases, blocks of IP addresses may be assigned to a subscriber.
- **Destination IP addresses** fall into the data retention scheme when they are associated with communications services such as email, messaging, chat, social media, forums, blogs, IP telephony (VoIP) and FTP at the time of receipt of a communication. Destination IP addresses associated with online browsing are excluded from the data retention scheme.
- **MAC addresses** are used to uniquely identify the network interfaces of each device on a local network segment and to facilitate directed communications

between devices on a local network segment. MAC addresses can be used to identify either a physical interface such as those on a wired Local Area Network or a radio interface such as those on a Wi-Fi network.

- **International Mobile Equipment Identity (IMEI)** numbers are unique to each mobile device. The IMEI can be used by the network provider to identify valid devices on the mobile network.
- **International Mobile Subscriber Identity (IMSI)** numbers are unique and used to identify the subscriber on mobile networks. The IMSI is stored on the SIM card. The SIM card can be transferred between devices.

UNCLASSIFIED

Communications data – examples

Categories	Reference in the Data Retention Bill	Reference in the former European Data Retention Directive	Examples from the dataset
Information about the communication *(services)*	The source of a communication (187A(2)(b))	5(a) data necessary to trace and identify the source of a communication	• The IP address assigned by an ISP to an internet access account or service. • Telephone numbers called or texted and associated IMSIs. • Email addresses and associated IP addresses. • VoIP identifiers and associated IP addresses. • Chat names and associated IP addresses. • The date, time and duration of a communication. • The type of communication (such as voice, SMS, email, chat, social media). • The type of service (such as Wi-Fi, ADSL). • Features of the service used during the communication (such as call forwarding).
	The destination of a communication (187A(2)(c))	5(b) data necessary to identify the destination of a communication	
	The date, time and duration of a communication, or of its connection to a relevant service (187A(2)(d))	5(c) data necessary to identify the date, time and duration of a communication	
	The type of a communication, or a type of relevant service used in connection with a communication (187A(2)(e))	5(d) data necessary to identify the type of communication	
Information about the parties *(users and devices)*	Characteristics of the subscriber of a relevant service (187A(2)(a)(i))	Telephony - 5(a)(1)(ii), 5(b)(1)(ii) Internet - 5(a)(2)(iii) , 5(b)(2)(ii)	• Name and address. • Postal and/or billing addresses. • Contact information, such as telephone number or email address. • Billing and payment information. • Account status and features. • Device identifiers such as IMEI and MAC addresses. • Identifiers for other services or devices linked to the same account. • Service specifications, including bandwidth, upload, and download volumes and allowances. • General location information—for example mobile telephone cell tower or Wi-Fi hotspot.
	Characteristics of an account relating to a relevant service (187A(2)(a)(ii).	Pre-paid mobile telephony - 5(e)(2)(vi)	
	Characteristics of a telecommunications device relating to a relevant service (187A(2)(a)(iii))	5(e) data necessary to identify users' communication equipment or what purports to be their equipment	
	The location of equipment, or a line, used in connection with a communication (187A(2)(f))	5(f) data necessary to identify the location of mobile communication equipment	

Table 1: Categories of communications data

UNCLASSIFIED

Executive Summary

The data retention bill is important to Australia's national security. It will provide ASIO with key capabilities to protect Australia in the information age. ASIO has persistently made the case for the intelligence value of retained communications data and the contribution it makes to reducing risk and preventing harm from national security threats. For example, communications data has been critical to the identification and disruption of all the planned mass casualty terrorist attacks in Australia since 2001.

The proposed dataset for mandatory retention is a compromise and balances several public goods, including security and law enforcement, human rights, and impost on industry. Consistent with the recommendations made in the committee's *Report of the inquiry into the potential reforms of Australia's national security legislation*, the data retention bill excludes communications content, continues the present controls that apply to communications data, excludes internet browsing, has a two year retention period, and continues oversight of ASIO's use of communications data by the Inspector-General of Intelligence and Security (IGIS).

ASIO has no argument with privacy requirements being be part of the TIA Act and that any exceptions must be grounded in law, with appropriate oversight, and fully accountable—as occurs now and as has occurred since the Act was introduced. Over that time, there have been no instances of deliberate misuse or abuse of the TIA Act by ASIO. On the small number of occasions where errors are made, the IGIS reports them to Attorney-General, and to the Parliament of Australia and public in her annual report. ASIO is not seeking to weaken such privacy protections and accountability.

Individual human rights (such as privacy) and collective community rights (such as a secure and safe environment) are indivisible and work to sustain each other. In ASIO's view, the present regime for regulating ASIO's use of communications data and the one proposed by the data retention bill take the right approach in relation to individual rights and collective community rights.

- Should the data retention bill be enacted, ASIO will continue to be required to seek a warrant to intercept communications, to access stored communications (such as emails or SMS messages), to remotely listen in on communications, or to precisely track individuals.
- The same legislative regime will continue to provide for a lower level of authorisation when ASIO requires access to communications data, recognising that such data only enables inferences to be drawn about the meaning of related

communications or the location of individuals. The vital intelligence value comes through ASIO correlating communications data with other intelligence available to ASIO.

In addition, public debate regarding the data retention bill focuses largely on the two year retention period, the retention of location information, and the security of the data. ASIO's positions in relation to these key issues are:

- A two year retention period is a compromise from ASIO's perspective – we would prefer a longer retention period due to the long-term nature of some security threats, the sophistication of foreign intelligence actors, and that intelligence lead information can surface many months or years after an event has occurred. For example, leads to individuals who have recruited spies or facilitated individuals to terrorist training camps require ASIO to examine historical connections to understand those they may have influenced to engage in activities prejudicial to Australia's security.

- The *where* of a communication is a vital piece of information that can inform security investigations in a number ways. For example, whether communications are domestic or international, the locality of the communication, and the coincident presence of several people in the same vicinity are all useful . The bill will not require providers to retain all location information – for example, GPS information and the non-communication network connections that mobiles make to cell towers are not required to be retained. What the bill requires is for providers to retain location information when communications occur – for example, what cell tower did an individual's mobile connect to when they made a call. This does not amount to tracking as some people have suggested. If ASIO has a requirement to monitor individuals, other capabilities can be deployed including tracking devices under warrant.

- ASIO will contribute to the work of government agencies in working with the telecommunications industry to secure their networks. The government has also noted that it is actively considering enhancements to telecommunications security.

However, there are misconceptions fostered by some in the public discussion about the use for intelligence purposes of communications data.

- ASIO does not have the resources, the need, or the inclination to undertake the large-scale mass gathering of communications data often alluded to in the public sphere. The IGIS also provides independent assurance to the Attorney-General, Parliament of Australia, and the public that ASIO does not engage in such activities.

- In any one year, a very small minority of the Australian community (a few thousand people at most) come to ASIO's notice through security investigations, inquiries and leads; multiple requests for access to basic communications data are required in most of these cases. Of this minority, only a small proportion may be suspected of seeking to do actual harm to Australia, its people or its interests. It is this small proportion who may be subject to more intrusive investigation, including using special powers under warrant where needed.

Certainly, the expectation from government and the majority of the Australian community is that ASIO must use all the tools at its disposal in an appropriate fashion where real harm is in prospect and needs to be prevented as well as in other matters in pursuit of its statutory functions. In doing so, ASIO contributes to a safe and secure environment in which the nation, individuals and our democratic institutions can operate freely and prosper. Nevertheless, balancing public safety and individual liberty always have been—and it is appropriate that they always will be—the subject of ongoing debate. The governance arrangements in place mean communications data is only sought by ASIO where it is required to resolve a security matter and is done so minimally.

Some legislative modernisation, however, is needed. Without it, developments in the telecommunications environment will continue to have detrimental consequences not only for Australia's national security and law enforcement capacities, but for individual privacy. ASIO supports revision of the legislation on the basis of these principles:

- The legislation should be overall technology-neutral without having to be revised for every new development in telecommunications technology;

- Carriers should retain communications data with access for ASIO and law enforcement agencies to continue to be in accordance with the TIA Act, rather than a central government-controlled repository of the data;

- Improvements should be made to the law to enable ASIO and law enforcement agencies to perform their functions more efficiently by reducing unnecessary bureaucratic overlay.

In ASIO's view, the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 will meet these aims and continue to enable ASIO to do its vital work in protecting Australians from harm. This submission explains how and why the collection and analysis of specific communications data is vital to the fulfilment of ASIO's national security responsibilities and how it is often used to limit the need to resort to more intrusive methods of intelligence collection.

Part 1 – Answers to the committee's questions

On 4 December 2014, the chair of the committee wrote to the Director-General of Security seeking information in relation to a series of ten questions. ASIO's response to each question appears below.

1. ***In each of the last five years, how many times has your agency sought a stored data warrant?***
2. ***In each of the last five years, how many times has your agency obtained a stored data warrant?***

ASIO is addressing questions 1 and 2 in the same answer.

The TIA Act does not establish a particular type of warrant to authorise ASIO to access stored communications. Rather, the TIA Act provides that an interception warrant issued to ASIO under Part 2-2 of the Act also authorises access to a stored communication if certain conditions are met. Specifically, section 109 of the TIA Act provides that ASIO is authorised to access a stored communication under an interception warrant issued to ASIO pursuant to Part 2-2 of the TIA Act if the interception warrant would have authorised interception of the communication if it were still passing over the telecommunications system. ASIO has accessed stored communications under an interception warrant infrequently in recent years, as shown in Table 2 (redacted from the public submission to avoid prejudicing national security).

In addition, Part 3-1A of the TIA Act enables ASIO to issue a domestic preservation notice to a carrier, which requires the carrier to preserve all stored communications that the carrier holds that relate to the person or the telecommunication service specified in the notice. There are two types of domestic preservation notices:

- historic preservation notices, which cover stored communications held by the carrier on a particular day; and
- ongoing domestic preservation notices, which cover stored communications held by the carrier in a particular 30-day period and for example can be used to prevent carriers from ageing off stored communications content (under normal business practices) before a warrant to access that content can be obtained.

ASIO may issue a domestic preservation notice in accordance with section 107H of the Act. ASIO is required to obtain an interception warrant in order to access the stored communications that are held by a carrier pursuant to a domestic preservation notice. Table 3 (redacted from the public submission to avoid prejudicing national security) provides the number of preservation notices ASIO has sought and obtained for each of the last five years.

ASIO's use of preservation notices is overseen by the IGIS who reported in her most recent annual report that 'Throughout the reporting period there was a very small number of such notices raised by ASIO. These activities were reviewed as part of our ongoing inspection program and there were no issues of concern identified in relation to those review.'(p.21).[1]

3. In each of the last five years, how many times has your agency sought authorisations for historical telecommunications data?

When approaching historical telecommunications data, ASIO does not submit requests for information that it knows does not exist. **Text redacted to avoid prejudicing national security.** Some service providers publish catalogues detailing the various types of communications data access requests that they are able to support and any limitations in terms of the scope, detail and depth of history that may apply.

Table 4 (redacted from the public submission to avoid prejudicing national security), provides the number of communications data requests ASIO has made under s175 of the TIA Act in each of the last five years. These figures are not published publicly because ASIO is exempt from doing so under s306 and s308 of the *Telecommunications Act 1997* from reporting requirements.

The number of requests does not reflect how many unique identifiers or subjects have been investigated. Due to the proliferation of service providers (as illustrated in Figure 1 on page 20), multiple requests need to be made depending on the intelligence required. So a subscriber check is less complex than understanding the transfer of communication services across providers. A request for communications data relating to four mobile numbers could generate approximately 40 separate requests in order to sufficiently cover all request types across the major providers, while a request relating to one email account may result in just one request.

Some simple requirements that generate requests to multiple providers are…

Text redacted to avoid prejudicing national security

- Such examples highlight the complexity of communications networks and effort required of ASIO to pursue security leads.

Whilst the level of requests has remained fairly constant over the last five years, the demand for communications data in security investigations has grown in parallel with society's use of digital and online technologies. There has been an increase in the number of communication devices and services used by subjects of

[1] The IGIS 2013-14 annual report is available online from http://www.igis.gov.au.

investigations, with the requirement to send requests to multiple providers to identify the user. At the same time, the growth in requests has been offset by industry changes and the reduced value of some communications data…**text redacted to avoid prejudicing national security.**

4. ***For each of the last five years, what percentage of historical telecommunications data which access was sought was:***

    a. ***Less than three months old;***

    b. ***Three to six months old;***

    c. ***Six to nine months old;***

    d. ***Nine to twelve months old;***

    e. ***More than 12 months old.***

Text redacted to avoid prejudicing national security. Requests that do not have a time component (such as certain email subscriber checks or due to legacy system limitations) have not been included in these figures. **Text redacted to avoid prejudicing national security.** Tables 5 and 6 (redacted from the public submission to avoid prejudicing national security) provide the data of interest.

Our informed observation in relation to Tables 5 and 6 is that the data is not representative of ASIO's security requirements in isolation but has been strongly shaped by ASIO's knowledge of industry retention practices and to meet industry requirements. Most importantly, each investigation is different and the value of data aged up to 24 months cannot be measured equally. Data over 12 months of age is often of great value for the reasons detailed in Parts 3 and 4 of this submission and illustrated by case studies 11-13—in short, retained data older than 12 months is deployed when other intelligence methods are not available to counter long-term, complex threats, especially from hostile intelligence services.

5. ***For each of the last five years, what percentage of historical telecommunications data actually used by your agency in its operations was:***

    a. ***Less than three months old;***

    b. ***Three to six months old;***

    c. ***Six to nine months old;***

    d. ***Nine to twelve months old;***

    e. ***More than 12 months old.***

In accordance with the legislated framework, all disclosures sought by ASIO were in connection with the performance by the organisation of its functions.

6. ***In approximately how many cases over the last five years did access to historical communications data accessed by your agency assist in preventing a serious crime from occurring?***

    a. ***If historical data was useful in preventing crimes from occurring, please provide examples which illustrate the use to which the historical data was put (without identifying specific individuals involved).***

    b. ***If historical data was useful in preventing crimes from occurring, approximately how old was the specific data that was of use in those instances?***

ASIO's role is intelligence-based and advisory and our law enforcement partners will be better placed to address this question.

7. ***In approximately how many cases over the last five years did access to historical communications data accessed by your agency assist in preventing a terrorist act from occurring?***

    a. ***If historical data was useful in preventing a terrorist act from occurring, please provide examples which illustrate the use to which the historical data was put (without identifying specific individuals involved).***

    b. ***If historical data was useful in preventing a terrorist act from occurring, approximately how old was the specific data that was of use in those instances?***

Communications data is used in almost every ASIO security investigation, including those directed at countering terrorism. The case studies in Part 4 of this submission detail specific examples where communications data has been used in ASIO's counter-terrorism investigations, including where more than two years of data has been needed.

Presently, there are over 300 counter-terrorism investigations, of which a third are high threat priority cases. High threat cases are ones in which ASIO holds credible information requiring time critical action to resolve or monitor. The dominant theme across these cases is the conflicts in Syria and Iraq. ASIO has identified around 70 Australians fighting with or supporting Islamic extremist groups in these conflicts, most are affiliated with Jabhat al-Nusra (JN) or Islamic State of Iraq and the Levant (ISIL). Around another 110 people here in Australia are actively supporting these groups, providing funding for them, recruiting for them, or seeking to travel to join them.

Over the last five years ASIO has provided the Minister for Foreign Affairs with security assessment advice recommending the cancellation of 124 passports, with nearly 100 of these done since mid-2011 in relation to Australians who have travelled, or intend to travel, to Syria or Iraq to engage in terrorism. Most recently, ASIO has suspended two passports of individuals believed to be intending to travel to Syria or Iraq. Communications data has been used in each of these cases, with some examples below, as well as another example relating to a person who had already travelled.

- Example 1: communications data was used to identify a falsely subscribed telephone used by an extremist intending to travel to Syria. This enabled investigative effort, which included other intelligence tools, directed at preventing his travel. When he attempted to depart for Syria his passport had been cancelled on ASIO's advice and he was stopped at the airport.

- Example 2: **Text redacted to avoid prejudicing national security.**

- Example 3: communications data was used, alongside other information, to confirm intelligence two Australians had sold their possessions and travelled to Syria with no intent of returning.
- Example 4: **Text redacted to avoid prejudicing national security.**

In these examples of disrupting travel to engage in terrorism overseas, the historical communications data used was no more than 3 months old.

8. In approximately how many cases over the last five years did historical telecommunications data accessed by your agency assist in securing a criminal conviction?

a. If historical telecommunications data did assist in security a criminal conviction, please provide examples which illustrate the use to which the historical data was put (without identifying specific individuals involved).

ASIO's role is intelligence-based and advisory and our law enforcement partners will be better placed to address this question.

9. Please describe in detail the use made of historical telecommunications data (as distinct from surveillance material and stored data obtained under warrant) in the investigation and prosecution of suspects in the following investigations:

a. Holsworthy Barracks (Operation Neath)

b. Benbrika and others (Operation Pendennis)

c. Lodhi and Willie Brigitte.

Historical telecommunications data was used extensively by ASIO in the relevant security investigations for these cases. These cases are also individually described in Part 5 of this submission. Some of the detail in relation to the use of communications data in these cases has been redacted from the public submission to avoid prejudice to national security.

Historical call records were acquired on each of the main subjects of interest of these investigations both prior to transitioning to warranted interception as well as in parallel to interception in cases where subjects were suspected of having multiple and/or falsely subscribed services.

In addition to the main subjects of investigation, historical call records were acquired on secondary persons of interest to determine their relationship to the main subjects and their role in the network. Through this investigative process, along with intelligence derived from other sources, secondary subjects often became primary subjects and subject to special powers warrants.

- In the case of Brigitte/Lodhi historical call records were acquired for services used by ...t**ext redacted to avoid prejudicing national security.**
- For Operation Pendennis historical call records were acquired for services used by...**text redacted to avoid prejudicing national security.**
- For Operation Neath historical call records were acquired for services used by... **text redacted to avoid prejudicing national security.**

Historical call records, in all cases, were used to:

- Develop a baseline understanding of the subject's contacts and general areas of movement, particularly contact with persons already known to ASIO.
- Identify overseas contacts.
- Assess the subject's relationship to primary subjects or their role within the network.

Text redacted to avoid prejudicing national security.

- Identify new contacts or contacts of security relevance, such as contact with chemical companies in the case of Operation Pendennis.

Text redacted to avoid prejudicing national security.

It is also important to note that communications data was also used to exclude individuals from investigations. ASIO is generally very conscious that the activities of a person may appear concerning until properly investigated and of the related obligation to protect a person's identity and reputation while an investigation is underway. ASIO pays particular attention to determining whether a person (or group) is undertaking activities relevant to security. Security inquiries more often than not determine that a person is actually not a security threat and are exculpatory in nature.

10. Why is there a significant discrepancy in the number of authorisations to access telecommunications data reported annually to the Parliament under the Telecommunications Interception Act, in contrast to the figure reported to the Australian Communications and Media Authority?

The Attorney-General's Department has the lead in relation to this matter. ASIO's requests for communications data are not reported in the annual report referred to in this question, leading some to speculate that requests made by ASIO are the reason for the discrepancy – ASIO can reassure the committee that this is not the case.

Part 2 – The need for legislative modernisation

ASIO's view remains that data retention is an important element of modernising the telecommunications legislative regime so as to regain vital intelligence capability. The data retention bill will:

- Enable national security and law enforcement agencies to continue to access communications data from providers.
- Provide appropriate accountability and oversight, including in ASIO's case continuing the existing accountability through the Attorney-General and the IGIS.
- Confirm industry obligations to provide communications data assistance, having regard to the dramatically changed telecommunications environment, and set technology-neutral standards for which communications data is to be retained.

Changes in the communications environment

The TIA Act and the *Telecommunications Act 1997* regulates access to communications data within Australia. These Acts are over 30 and 15 years old respectively and are based on the technologies and business practices at that time. In ASIO's evidence to the committee's *Inquiry into Potential Reforms of Australia's National Security Legislation*, as well as in evidence to the Senate Legal and Constitutional Affairs Committee's *Inquiry into a Comprehensive Review of the TIA Act*, ASIO noted the changes in communications since these laws were introduced and that the assumptions underpinning them no longer apply.

Online communications are now part of a vibrant society in ways that were not anticipated in 1979. Today's telecommunication services are simultaneously global and local, with offshore-based network infrastructure delivering services onshore. Most Australian citizens use several communication services in their day-to-day lives, such as fixed line, mobile networks, and free Wi-Fi, and use multiple communications applications over these services including email, chat, instant messaging, VoIP, social media and file sharing. This evolution in complexity is illustrated by Figure 1 (on page 20).

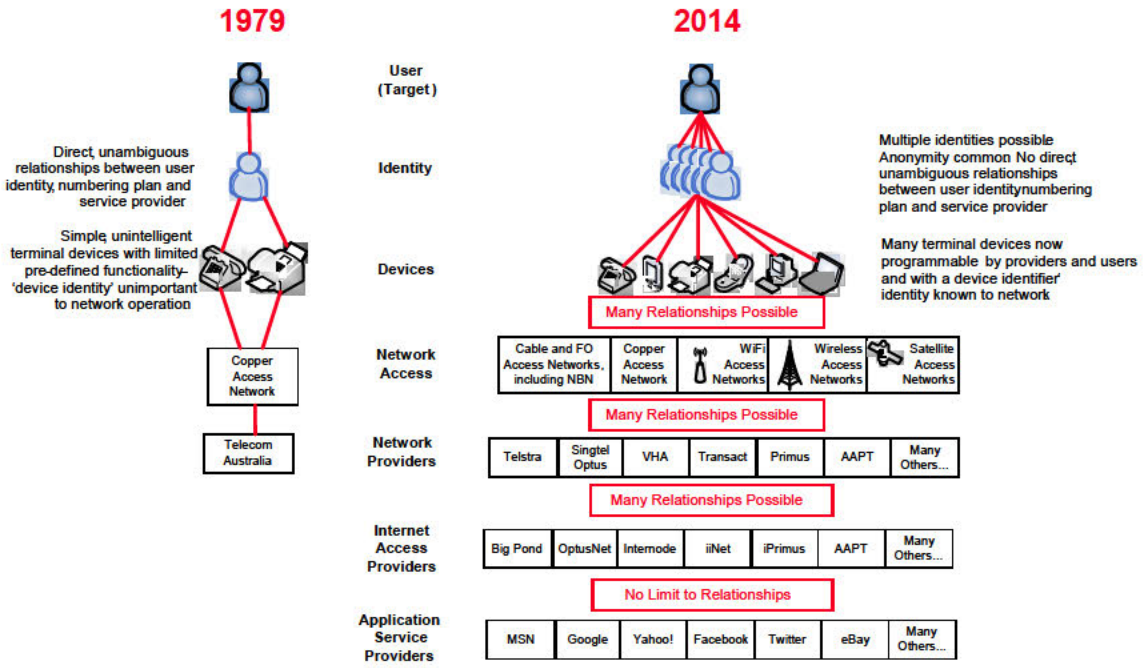

Figure 1: Evolution in Australia's telecommunications environment

The business practices of the telecommunications and internet service industry have also changed to match the differentiation in communication services and applications. For example, there has been a trend of providers moving to volume based monthly plans, with no business need to retain data for individual communications. In essence, telecommunications providers only need to know in the moment where to send a communication and to whom it should be sent; some providers only retain the details of the amount of data sent for their billing purposes.

During the December 2014 hearings, the committee sought agency views on whether retention periods should be consistent across categories of historical communications data – between telephony and IP-based data. In ASIO's experience the retention period for historical communications data are variable across service providers as shown by the example retention periods in Table 7.

Historical communications data	Range of retention
Subscriber information – name and address	7 years or longer
Telephone numbers called/received	6 weeks to 7 years
Telephone numbers associated with SMS	60 days to 7 years
Mobile Handset and SIM data	Up to 7 years
IP account, device and address information	90 days to 3 years
Addresses associated with email and other IP communications	45 days to 3 years

Table7: Ranges of retention by service providers of historical communications data

The retention period for IP-based data is particularly volatile and tends to be weeks and months rather than years. In the near term all the historical communications data will be IP-based due to the uptake of IP-based technologies by telephony providers, characterised by the further fragmentation of communications across multiple providers.

With this in mind, it is important that the legislation remain technology neutral and that there should be a single retention period across the board, with a particular need to increase the retention period for IP-related data from present arrangements. The suggestion that there could be different retention periods reflects the position the data retention bill is seeking to move away from of inconsistencies between legacy telecommunications systems that kept everything (PSTN telephony) and new systems that ideally keep almost nothing (IP-based). Communications data that does not resolve to a transaction (which is where the technology is heading) is not of significant value to service providers but it can be to ASIO and law enforcement agencies. ASIO's core requirement is ongoing access to such data with a mandated retention period across industry that applies to a defined set of historic telecommunications data.

These realities mean there is a real risk, unless there is modernisation of the legislative regime to mandate retention of communications data, that law enforcement and national security agencies will progressively become blind to the digital tracks left by serious crimes and national security threats – coined by some as the 'going dark' problem. The committee has already recognised the reality of this challenge for Australian agencies when it concluded:

> 'There is no doubt that the enactment of a mandatory data retention regime would be of significant utility to national security agencies in the performance of their intelligence, counter-terrorism and law enforcement functions. As well, it is clear that changes in the data retention practices of telecommunications providers mean that much data which was previously retained, in particular for billing purposes, is no longer retained; this has resulted in an actual degradation in the investigative capabilities of the national security agencies, which is likely to accelerate in the future.' (p.190). [2]

This is not unique to Australia – it is an international challenge (see Box 1 and Box 2 on pages 22-23) – and the concerns are not limited to government. For example, the International Chamber of Commerce (ICC) has issued policy statements in 2010 and 2012, *Global business recommendations and best practices for lawful interception requirements* and *Using mutual legal assistance treaties (MLATs) to improve cross-border lawful intercept procedures*. Whereas the 2010 statement was focussed solely on interception of content, the 2012 statement evolved to include a recommendation in

[2] See paragraph 5.207 on page 190 of the Parliamentary Joint Committee on Intelligence and Security May 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*.

relation to communications data and the need to identify the source and destination of communications across global networks.[3] Both policy statements accepted the need for government to have investigative capabilities across borders in a world of global communications.

Box 1 – Overseas approaches to data retention: United States

In the United States congressional hearings in 2011 directly considered the challenge in the *Going dark: lawful electronic surveillance in the face of new technologies* hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee of the Judiciary, House of Representatives. The Federal Bureau of Investigation detailed the challenges it faces during that hearing,[4] and they persist as outlined in an October 2014 speech by the FBI Director to the Brookings Institute.[5]

In the wake of the Snowden leaks, President of the United States of America, Barak Obama, referred to the challenges faced by law enforcement and intelligence agencies[6] and established a review group to look at intelligence access to and the collection of communications data. Following the review, in January 2014, President Obama issued a Presidential Policy Directive that was intended to change the manner in which data is collected, stored and accessed by the US intelligence community.

In March 2014, President Obama announced that the communications data should remain held by providers with a legal mechanism enabling the intelligence community to access it and in May 2014 the US House of Representatives passed the USA Freedom Act that created this mechanism. The US Senate has since introduced a bill to ban bulk collection of data, which has bipartisan support and is supported by the Department of Justice and the Director of National Intelligence.

[3] The policy statements are available online from the International Chamber of Commerce's website: www.iccwbo.org.

[4] See FBI evidence and the hearing transcript for more detail, available online: www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies; and www.gpo.gov/fdsys/pkg/CHRG-112hhrg64581/html/CHRG-112hhrg64581.htm.

[5] Director Comey's speech is available from www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[6] The United States President's 17 January 2014 remarks are available online from www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

Box 2 – Overseas approaches to data retention: Europe and the United Kingdom

Europe

The European Union (EU) Data Retention Directive (2006/24/EC of 15 March 2006) provides another international model for mandatory data retention. Much has been made of the April 2014 decision of the European Court of Justice relating to the Directive. The Court's concern with the EU scheme, and why the Directive was held to be invalid, was not about data retention but about the safeguards in place. The European Commission, and many European countries, is actively working to address these issues, as shown by the United Kingdom passing laws to maintain its practices.

The reason European policymakers are working to address the issues is because the data retention system has been shown to be effective. In 2011, the European Commission prepared an evaluation report on the effectiveness of data retention.[7] That report concluded that the EU should support data retention as a security measure, finding that *'the evidence… attests to the very important role of retained data for criminal investigation'*, and *'These data provide valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Their use has resulted in convictions for criminal offences which, without data retention, might never have been solved. It has also resulted in acquittals of innocent persons.'*

United Kingdom

In the United Kingdom the Intelligence and Security Committee of Parliament considered the issues in its report on *Access to communications data by the intelligence and security agencies*. The committee recently reiterated its conclusion from that report in its November 2014 *Report on the intelligence relating to the murder of Fusilier Lee Rigby* and found that '…it is essential that the Agencies maintain the broad capability to access communications data.' (p.139). [8]

Following the 2013 report of the Intelligence and Security Committee of Parliament, the Data Retention and Investigatory Powers Act was subsequently passed and came into effect on 18 July 2014. It provides powers to introduce secondary legislation to replace the Data Retention Regulations, while providing additional safeguards in response to the European Court of Justice judgment of 8 April 2014 which declared the Data Retention Directive invalid. It clarifies the nature and extent of obligations that can be imposed on telecommunications service providers based outside of the UK under Part 1 of the Regulation of Investigatory Powers Act 2000 ('RIPA'.) The Act ensures that, as the original legislation intended, any company providing communication services to customers in the UK is obliged to comply with requests for communications data and interception warrants issued by the Secretary of State, irrespective of the location of the company providing the service.

[7] More information on the European approach to data retention, including milestone documents such as the Data Retention Directive, case studies, and the evaluation report can be found at the European Commission's Directorate-General of Home Affairs website on data retention: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm.

[8] The committee's reports are available online from isc.independent.gov.uk/committee-reports/special-reports.

Security challenges persist

The above trends in communications practices are becoming far more significant in the current security environment.

- Australia remains a terrorist target. In September 2014, based on advice from ASIO, the Government raised the National Terrorism Public Alert level from MEDIUM to HIGH. ASIO's advice reflected a body of intelligence pointing to the increased likelihood of a terrorist attack in Australia, including concern about the increasing number of Australians connected with or inspired by terrorist groups such as ISIL, Jabhat al-Nusrah, and al-Qa'ida.

- Espionage activity against Australia persists. In the context of telecommunications systems, a particular vector of concern is cyber attacks. Both government and industry systems are being targeted by cyber attacks from hostile foreign powers, which are using this means to seek access to privileged political, military, economic, trade, business, and government information with a view to undermining Australia's security and prosperity.

- The leaks of former NSA contractor Edward Snowden have also had effects, including public reporting suggesting the level of encryption on the internet has increased substantially.[9] In direct response to these leaks, the technology industry is driving the development of new internet standards with the goal of having all Web activity encrypted, which will make the challenges of traditional telecommunications interception for necessary national security purposes far more complex.

The Government and Australian communities continue to expect ASIO to protect Australia, its people, and interests from such threats in the changing technological and social environment. It is a fact that the connectivity and interactivity afforded by online networks and applications is as much of a driver of those who would do us harm as it is of innovation and economic growth. For example:

- Social media is driving Australians to participate in the conflicts in Syria and Iraq and engage in terrorism there, it is enabling Australians to be extremist propagandists, and is inspiring individuals in Australia to violence. [10]

- Online anonymity, in addition to the above activities, otherwise separates people from the consequences of their actions, with one security outcome being

[9] For example see www.sinefa.com/encrypted-traffic-grows-post-edward-snowden-nsa-leak
[10] See then Director-General of Security, Mr David Irvine's 12 August 2014 address to the Australian Institute of International Affairs, available from www.asio.gov.au.

individuals prepared to leak classified information on the Internet, or make reference to classified material when communicating online.[11]

- The range, scale and sophistication of state actors engaged in hostile cyber activity against Australian systems continue to increase.[12]

Community perceptions of security intelligence

There are some public misconceptions regarding data retention, including that ASIO is seeking direct access to the communications data of all Australians. This is not the case. ASIO's position has consistently been that:

- The communications data should continue to be stored by the provider or ancillary service provider;
- ASIO requires access to retained communications data to enable it to pursue national security matters (and only those matters);
- Requests for communications data will only be made by ASIO after a duly authorised and documented process; and
- The IGIS must continue to provide formal oversight of ASIO's requests for data, access to it, and use of it.

However, there are indications from polls that the Australian community understands the significance of security intelligence threats to Australia, the need to consider both privacy and the need to protect the community, and that the community is not as concerned about government surveillance as some might think. The Lowy Institute for International Policy asked people to rate a list of possible threats to Australia's, in its February 2014 survey of 1150 Australians.[13] International terrorism and cyber attacks from other countries were identified as critical or important threats by 94 per cent and 88 per cent of respondents respectively. The 2013 Lowy Poll also sought people's views on the Australian Government's measures to combat terrorism, in its March 2013 survey of 1002 Australians.[14] It found that the majority of those polled—80 per cent—accepted the need for the some imposition on individual rights in dealing with terrorism. Sixty- eight per cent agreed that 'The government has struck the right balance between protecting the rights of citizens and fighting terrorism' and 11 per cent believed that 'The

[11] See 'The trusted insider – why people turn', ASIO Deputy Director-General Kerri Hartland's 23 May 2014 address to the Critical Infrastructure Resilience Conference. The speech is available online from www.asio.gov.au.
[12] For more information on see the 'Security Environment and Outlook' section of the ASIO Report to Parliament 2013-2014, available from www.asio.gov.au.
[13] The Lowy Institute's poll is available from www.lowyinstitute.org/publications/lowy-institute-poll-2014.
[14] The Lowy Institute's poll is available from www.lowyinstitute.org/publications/lowy-institute-poll-2013.

government leans too much toward protecting the rights of citizens over fighting terrorism'. Nineteen per cent believed the opposite.

Also, the Office of the Australian Information Commissioner sought the views of Australians on the biggest privacy risks in its June–July 2013 survey of 1000 Australians for its Community attitudes to privacy report.[15] People could nominate several privacy risks.

- The report found concerns about online services/social media (48 per cent), identity theft/fraud (23 per cent), data security/data breaches (16 per cent) and financial details/information/fraud (11 per cent) were perceived as the biggest risks.

- Surveillance (4 per cent), government information sharing/information collection (3 per cent), and unauthorised monitoring of information/data mining (1 per cent) were not perceived by many of those polled as the biggest risks.

- The survey also found government departments ranked third as organisations trusted to protect personal information. This was behind health service providers and financial institutions, and ahead of insurance companies, charities, technology companies, retailers, real estate agents, debt collectors, market researchers, the e-commerce industry, and social media organisations.

In November 2014, after the data retention bill had been introduced to The Parliament of Australia, Essential Research sought people's view on how much trust they had in organisations to store their personal data safely. They surveyed 1003 Australians online between 7-10 November. The report found the greatest trust in agencies such as AFP and ASIO, with 53 per cent of respondents having a lot or some trust in those agencies. However, in the same survey, opinion was divided as to the value of government agencies having access to communications data to protect society or whether it was going in the wrong direction.[16]

[15] The Office of the Australian Information Commissioner's report is available online from www.oaic.gov.au/privacy/privacy-resources/oaic-community-attitudes-to-privacy-survey-research-report-2013.
[16] The Essential Report is available online from www.essentialvision.com.au/categories/essentialreport.

Part 3 – The value of data retention

ASIO relies on communications data in pursuing security investigations that reduce the risk to Australia, its interests and its people. ASIO supports the retention of the data provided for in proposed section 187A. Consistent with our long-standing public position on the need for modernisation of the TIA Act, the bill will:

- ensure ASIO and law enforcement agencies can continue to access communications data to perform their functions and protect Australians;
- describe clearly what communications data should be retained, without being exhaustively prescriptive or tied to specific technologies;
- require telecommunications providers to retain data for two years.

The committee has recognised that the challenge posed by 'going dark' is not a set of hypothetical scenarios. To restate the degradation in capability security and law enforcement agencies are no longer able to:

- **reliably identify communicants** of interest and associate them with services and applications—this is a consequence of anonymous access to telecommunications services and impediments to access of user records;
- **reliably and securely access content and communications data** within the networks—brought about by common use of encryption, globalisation, industry outsourcing, and industry non-compliance with interception capability obligations; and
- **extract intelligence or evidence** by reconstructing the communications—this is a consequence of the increasing complexity of internet protocol communications, widespread use of encryption and increasing data volumes.

The government's proposed mandatory data retention regime will, to some degree, reduce these gaps and mitigate, in part, the risk of information not being available to inform intelligence and actions to protect Australians and Australian interests.

What communications data does ASIO need for its work?

The type of communications data ASIO is seeking to be retained under a mandatory retention scheme for national security purposes is shown in Table 1 on page 7, and as can be seen from the table our minimum requirements align with the information proposed to be retained by the bill. ASIO recognises that the proposed dataset for mandatory retention is a compromise and balances several public goods, including security and law enforcement, human rights, and impost on industry.

Why is a two year retention period necessary?

The committee considered the length of time industry should retain communications data for in its *Inquiry into Potential Reforms of Australia's National Security Legislation* and recommended a retention period of no more than two years.

ASIO supports two years as a minimum retention period, and would prefer a longer period. This is because, while some security investigations are a retrospective examination of a specific incident, foreign states engaged in clandestine activities against Australia take a long-term, strategic approach to espionage so as to avoid their activities being detected. ASIO deploys investigative tools and techniques that match the nature of this risk, including analysis of trends over extended periods to baseline activities and enable threats to be identified by proxy through anomalies in patterns of behaviour.

- ASIO often relies on the analysis of communications data in the early stages of an investigation to assist in quickly assessing the likely security significance of an investigative lead and the likely extent of the service user's involvement in activities of potential security concern. This minimises the use of other collection techniques which are more intrusive and expensive. Such lead development use is common across ASIO's security investigations and involves requests for communications data over short timeframes.

- From a counter-terrorism perspective, longer term analysis of contacts has value. For example, the presence of specific contacts in the earliest stages of radicalisation – influential recruiters, radicalisers, and facilitators – can provide insight as to the radicalisation or extremist trajectory that an individual is on, their likely peers and courses of action they may have a propensity to embrace. These contacts, having introduced the individual to a more extremist network, consider their work done and may no longer be present in current contact data. A two year window is important when assessing an individual's adoption of an extremist agenda.

- From a counter-espionage perspective, records of historical contacts can also provide very high value. Once recruited by a foreign government, an individual will usually then employ some measure of tradecraft to ensure a greater degree of communication security. However, the adoption and observance of such practice is rare, hence that record of historical contact providing important lead intelligence. Also, often in espionage investigations there is no known or specific incident or starting point. ASIO must baseline the activities and threat posed by adversaries over an extended period in order to identify indicators, and once relevant indicators are found look again over time to understand the extent and

scope of the activity and harm – this cannot be done if the communications data is not retained.

- For example...**text redacted to avoid prejudicing national security.** Access to more than two years of historical communications data was vital in enabling ASIO to fully investigate this case and identify the network of contacts and the extent of harm posed to Australia's national interests over this period of time. Such patience by sophisticated nation state adversaries is common. The harm to Australian national interests by such operations can be catastrophic.

In addition to the above, a shorter period is problematic because it is not uncommon for intelligence leads about a key event to be received some time after it has occurred (see Case Study 1).

- For example...**text redacted to avoid prejudicing national security.**

What security outcomes are generated from communications data?
The unique effects that accessing and analysing communications data can achieve for security investigations includes understanding threats and developing leads, such as:

- providing advice of protective security measures than can be used to mitigate risk (see Case Study 1);
- identifying individuals who were previously unknown to ASIO, including those contacting individuals or communications services of security interest to ASIO (such as known foreign intelligence actors, or offshore terrorists), or those who use communications services for activities relevant to security (such as making threats over the phone, advocating terrorism online, or uploading extremist videos to a file-sharing service) (see Case Study 2 and Case Study 7);
- identifying covert communications attempts, for example...**text redacted to avoid prejudicing national security** (see Case Study 3, Case Study 4, Case Study 5, and Case Study 7);
- extending understanding of the scope of threats and the harm they pose by reliably identifying the contacts and networks of individuals of security concern, including to rule out links to security activity (see Case Study 6, Case Study 7, and Case Study 9);
- understanding the development of threats before ASIO was aware of them to inform judgments of the harm and provide other security leads, including over periods greater than two years (see Case Study 10, Case Study 11, and Case Study 12).

These effects offer significant advantage to ASIO in detecting, understanding, and then defeating the actions of individuals, groups, and foreign states which deliberately seek to hide and obfuscate their activities from our view, including those who employ sophisticated methods to engage in espionage and foreign interference against the nation. Where communications data is partial or completely absent, the risk is raised because of partial knowledge of threats and harms **(**see Case Study 8). We also have an example of past success that could not be replicated because the communications data is not retained by the providers **(**Case Study 9**)**.

Many of these effects can only be achieved through retained historical data, rather than simply through requests for a data preservation scheme. A preservation scheme will work well to monitor known individuals from the preservation point onwards, but it cannot be used to identify individuals making threats online or uploading beheading videos. A preservation scheme without a reliable data retention scheme also falls short in failing to have the data available to enable a picture to be built of a network over time. This is important in analysis of the development and trajectory of security threats, including covert communications networks, as we see used by spies and have seen used in some of the attempted terrorist attacks in Australia, and in understanding the connections of all those involved in plotting (see case studies).

ASIO's use of communications data reduces the need for more intrusive, costly, and time consuming methods to inform judgments of an individual's relevance to security and whether they are engaged in activities prejudicial to security. The earlier ASIO can provide advice on security matters, the greater opportunities there are for preventative action to reduce the risk from security threats to Australia, its interests and its people. The case studies underscore this point, showing risk reduction in relation to terrorism and cyber activities.

Some of the case studies also show the inability to progress, or challenges in progressing, security investigations and highlights the challenge for ASIO in understanding the harm being done from security threats when communications data is not available.

Part 4 – Case studies

Case study 1: hostile foreign intelligence use of Australian telecommunications infrastructure for cyber espionage

Text redacted to avoid prejudicing national security.

Communications data has allowed ASIO to identify the intelligence goals and capabilities of hostile intelligence services, and the intelligence benefits derived from their cyber activities. Such insights enable victim notification, the strengthening of defensive responses and the identification and mitigation of the harm, as well as contributing to an assessment of the strategic priorities and capabilities of the foreign intelligence service.

In 2013 an internet service provider reduced its retention period for IP address allocation to individual customers from a period of many years down to three months. In the 12 months prior to that decision, 10 ASIO investigations required that information for periods older than three months. That information would have related to victims of cyber attack or people in Australia communicating with suspected or known terrorists.

In other cases, ASIO does not receive leads for several months after activities. A number of brief classified examples are provided below (removed from the public submission to avoid prejudice to security) to give a sense of timeframes associated with the lag between an event occurring, ASIO receiving lead information to inform an investigation, and the ability to then access relevant communications data.

Text redacted to avoid prejudicing national security.

- The risk of not being able to access carrier data to progress investigations of these types of sophisticated state-sponsored intrusions and targeting of Australian systems would be potential damage to national security.

Case study 2: links to Australia from a terrorist cell disrupted overseas

Following overseas intelligence operations that disrupted an active terrorist cell, a cooperating foreign liaison partner provided ASIO with an Australian telephone number. The number was with other telephone numbers connected to known supporters of the cell. No other details were provided.

ASIO sought data from telecommunications providers and identified the service subscriber. The individual was not the subject of current investigation. ASIO sought cooperation from the relevant carrier to provide copies of the service's telecommunications records. An analysis of this information showed the individual had dialed a range of overseas numbers known to be linked to individuals engaged in extremist activity. While the person was in regular contact with a number of individuals in Australia known to espouse extremist views, the analysis raised the priority of the individual and changed the focus of the security investigation.

This lead, and the context developed from analysis of telecommunications records provided the basis for a fuller and more intrusive warranted interception operation against that person. ASIO was concerned that a terrorist cell similar to the one disrupted overseas had formed in Australia or was in the process of forming. The group was indeed a dedicated cell and, while it had not progressed to specific terrorist planning, had been requested by its overseas counterpart to conduct a terrorist act in Australia. The group was effectively disrupted.

Case study 3: Prevention of terrorist attack - Operation Pendennis (Melbourne and Sydney)

In 2005 and 2006 a combined ASIO and law enforcement operation, Operation Pendennis, in Melbourne and Sydney prevented two mass casualty terrorist attacks in Australia and resulted in the arrest of 22 men. In Melbourne, 13 men were arrested. Two pleaded guilty to terrorism offences and were convicted, seven were found guilty and convicted of terrorism offences, and four were acquitted. Telecommunications content formed a substantial part of the prosecution cases. In Sydney, five men were found guilty by a jury of conspiring to prepare a terrorist act (and received prison sentences ranging from 23 to 28 years). They have appealed both convictions and sentences. Four other men pleaded guilty to lesser terrorism offences.

However, the investigations would never have reached the point of prosecution without the use of communications data. Historical call records were acquired for services used…**text redacted to avoid prejudicing national security**. Communications data was used to identify a covert phone network that was being used in an attempt to conceal activities from ASIO and law enforcement agencies. Had this data not been available, ASIO and law enforcement agencies would likely not have understood the activities of those involved in the planning of a terrorist attack in Australia.

Without access to this communications data, ASIO would not been equipped to provide advice to manage the risk and work with law enforcement partners to prevent a mass casualty terrorist attack in Australia. For example, communications data enabled ASIO to identify previously unknown contacts, including with…**text redacted to avoid prejudicing national security.** ASIO correlated such data with other intelligence sources to identify key events in the plot, such as…**text redacted to avoid prejudicing national security.**

Text redacted to avoid prejudicing national security.

The analysis of communications data is a key component in the overwhelming majority of priority security investigations and consistently proves to be an invaluable intelligence capability, including helping eliminate individuals from security concern.

Text redacted to avoid prejudicing national security.

Case study 4: Prevention of terrorist attack - Operation Neath (Melbourne)

On 4 and 5 August 2009, five Melbourne-based men were arrested and charged with conspiracy to commit an act in preparation for a terrorist act. The arrests resulted from a joint investigation by ASIO, the Australian Federal Police, Victoria Police and the New South Wales Police Service.

On 23 November 2010, three of the five were found guilty in the Victorian Supreme Court of conspiring to undertake acts in preparation for a terrorist attack – namely, planning an armed assault on Australian Defence Force personnel. On 16 December 2011 they were sentenced to 18 years' imprisonment. The other two individuals were found not guilty and released.

Communications data was used to identify connections between individuals, to analyse connections to other security investigations, to generate leads to overseas extremists, and to identify attempts by the individuals to hide their communications…**text redacted to avoid prejudicing national security.** Had this data not been available, ASIO and law enforcement agencies would likely not have understood the network of people that were involved in the plot.

Text redacted to avoid prejudicing national security.

Case Study 5: ***Text redacted to avoid prejudicing national security…*** *Australian extremist*

Text redacted to avoid prejudicing national security.

Twelve months of retained communications data from all major Australian telecommunications providers was collected on specific services and enabled ASIO to identify the users...**text redacted to avoid prejudicing national security…**Australian extremist.

Text redacted to avoid prejudicing national security.

- ASIO investigation has shown members of the family are supplying funds to Syrian extremist group Jund al-Sham which has sought formal affiliation with proscribed terrorist group Jabhat al-Nusra. **Text redacted to avoid prejudicing national security.**
- Without historic communications data, ASIO would likely not have been able to identify the users...**text redacted to avoid prejudicing national security…**and would not have any knowledge of the family's activities.

Case study 6: Identification of hostile cyber actors and understanding the harm

In one case, ASIO received lead information that individuals associated with the espionage program of another country had travelled to Australia some 18 months earlier. Communications data from that period enabled ASIO to identify the individuals, and contributed to an assessment of their activities, including that they had travelled to Australia, at least in part, to develop covert cyber espionage infrastructure.

In another instance, technical analysis identified a methodology used by a state-sponsored cyber espionage actor of which ASIO was not previously aware. Retention of telecommunications data enabled ASIO to identify previous instances of the cyber actor's targeting or use of Australian infrastructure. From this, ASIO developed its understanding and assessment of the cyber capabilities of the hostile country and the potential harm it was causing.

Case study 7: Disruption of terrorist attack - Brigitte/Lodhi (Sydney)

In September 2003 the French security service advised ASIO that French national Willie Brigitte had participated in training in Pakistan and/or Afghanistan and that they believed he had travelled to Australia in May 2003. ASIO, the Australian Federal Police and the New South Wales Police Service investigated and as a result Brigitte was identified, placed in immigration detention and removed from Australia to France. Two other individuals were arrested by the AFP on terrorism charges.

In June 2006, one of these individuals, Faheem Lodhi, was convicted by a jury of three terrorism offences and sentenced to 20 years imprisonment. The court determined it was likely he intended to use maps of the Australian electricity grid in a plan to bomb part of the grid. In December 2007, the NSW Court of Criminal Appeal dismissed Lodhi's appeal. In June 2008, Lodhi was unsuccessful in gaining special leave to appeal to the High Court.

In March 2007, a French court convicted Brigitte for planning terrorist attacks in Australia in 2003 in conjunction with Sajid Mir, suspected of being external operations leader for proscribed terrorist group Lashkar-e-Tayyiba.

Communications data and analysis was a key tool in identifying the group involved in the plot, which led to further intelligence which uncovered details of the plot and overseas links. Without the retained communications data, the plotters may not have been identified and disrupted.

- Historical call records were acquired for services used...**text redacted to avoid prejudicing national security.**

Text redacted to avoid prejudicing national security.

- Communications data also enabled ASIO to identify overseas contacts of those involved in the plot, including links to terrorist Sajid Mir, suspected of being Lashkar-e-Tayyiba's external operations leader.

Case Study 8: Missing data in investigation into hostile foreign intelligence activity

The text of these case studies has been redacted to avoid prejudicing national security.

Case Study 9: ***Text redacted to avoid prejudicing national security***

The text of these case studies has been redacted to avoid prejudicing national security.

Case Study 10: Use of more than two years of retained communications data to understand radicalisation pathways

Case Study 11: Use of more than two years of retained communications data to understand foreign interference

The text of these case studies has been redacted to avoid prejudicing national security.

*Case Study 12: Use of more than twelve months of retained communications data to understand…**text redacted to avoid prejudicing national security***

The text of these case studies has been redacted to avoid prejudicing national security.

Without retained communications data, ASIO would likely have had only limited windows into these harmful activities against Australia's interests.

Part 5 – Accountability and oversight arrangements

There are numerous controls on ASIO's activities, including ASIO's access to, use of, retention, and destruction of communications data.

In our submission to the Senate inquiry into a comprehensive review of the *Telecommunications (Interception and Access) Act 1979*, ASIO noted six guiding principles for ethical and effective intelligence surveillance that were articulated by Sir David Omand, a former Chairman of Britain's Joint Intelligence Committee:

- There must be sufficient sustainable cause;
- There must be integrity of motive;
- The methods used must be proportionate;
- There must be right and lawful authority, with accountability up a recognised chain of command to permit effective oversight;
- There must be a reasonable prospect of success; and
- Recourse to secret intelligence must be a last resort.[17]

These concepts are found within the oversight and accountability measures governing ASIO's approach to communications data.

- The ASIO Act regulates the purposes for which ASIO can collect, analyse, share, and report on intelligence, including in relation to communications data. The ASIO Act also prohibits the unauthorised handling or recording of national security information, including communications data obtained by ASIO. These offences were introduced recently by the *National Security Legislation Amendment Act (No. 1) 2014*.
- Guidelines issued by the Attorney-General to ASIO require our intelligence methods to be proportionate—and they are—and this directly applies to requests for communications data, with data requested only when we judge it will usefully progress a security matter. The Guidelines also require ASIO to use the least intrusion into individual privacy consistent with the performance of its functions and the requirement to use less intrusive methods before more intrusive methods. The Attorney-General has indicated that the Guidelines will be reviewed in 2015.

[17] Sir David Omand's article is available online via: www.theguardian.com/commentisfree/2013/jun/11/make-surveillance-ethical-and-effective.

- A case is made for why communications is required, and is documented, and approved—ASIO has detailed authorisation processes in place for requesting communications data, with higher levels of approval required for requests of prospective communications data.

- In practice, the process works as follows: having considered a submission from the investigating officer detailing the justification for the request, the approving officer directs that a formal written request be sent to the relevant service provider, which, in turn, will respond in writing. The telecommunications data relevant to that specific service which has been collected and stored for normal business purposes by the service provider is made available to ASIO under the TIA Act only on receipt of the formal request through established and secure mechanisms.

- ASIO has procedures in place to ensure the people of ASIO understand our legislation, internal policies and procedures, and accountability mechanisms. In short: what is allowable and what is not.

- ASIO's communications data requests are subject to ongoing, regular review by the IGIS, who provides independent assurance to the Attorney-General, to the Parliament and the public, including through an Annual Report to the Parliament.

    - The IGIS reported in relation to 2012–13 that ASIO's '…prospective data authorisations were endorsed by an appropriate senior officer, and that ASIO is using this method of inquiry responsibly, with appropriate internal controls.' (p.19).[18]

    - Likewise, the IGIS reported in relation to 2013-14 that '[she] did not identify any concerns with ASIO's access to prospective and historic telecommunications data. My office's oversight of this particular technique decreased during this reporting period due primarily to changes in our inspection program and the high rate of compliance in this area.' (p.21). [19]

- Finally, ASIO's security intelligence activities are prioritised on the basis of greatest or most immediate threat or harm. ASIO does not have the resources, interest, nor authority to engage in frivolous, wasteful, or irrelevant eavesdropping of the Australian community's private conversations.

[18] The IGIS 2012-13 annual report is available online from http://www.igis.gov.au.
[19] The IGIS 2013-14 annual report is available online from http://www.igis.gov.au.

Academics and thinks tanks have examined oversight of intelligence agencies in democratic societies, including standard controls that should apply, including in the publicly available report *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* published in 2005 by The Geneva Centre for the Democratic Control of Armed Forces, the Norwegian Parliamentary Intelligence Oversight Committee, and the Human Rights Centre of the University of Durham.[20] Consistent with the relevant best practices in that report relating to information collection and retention:

- ASIO's legislative mandate limits the purposes for ASIO to collect communications data;
- there is law providing controls for the use and sharing of such information;
- the Attorney-General's Guidelines (issued under the ASIO Act and tabled in Parliament) provide that ASIO only handle personal information if it is reasonably necessary for the performance of ASIO's functions and that records about a subject whose activities are no longer relevant to security are to be destroyed under disposal schedules agreed with the National Archives; and
- there is independent oversight of the adherence to these elements by the IGIS.

Under the proposed data retention scheme, what additional oversight or accountability measures would be required in relation to ASIO?

In ASIO's view, the present measures in place for access and use of communications data are appropriately regulated and there is no need for a shift to require a warrant for communications data. ASIO takes the existing legal framework and accountability measures seriously—it is in ASIO's interests in performing its statutory functions to have the confidence of the public and to be regarded as ethical and accountable. ASIO believes the appropriate consideration of national security and human rights, including privacy, is present in the current arrangements, including through ministerial accountability, review by the IGIS, oversight of this committee, and the functions of the Independent National Security Legislation Monitor. These mechanisms operate effectively and provide assurance to Government and the public of the legality and propriety of our work, including ASIO's use of communications data, so that we will continue to have legitimacy and support within Australian society.

ASIO supports the committee's previous recommendations relating to governance and accountability of any data retention scheme, including a review of the legislation

[20] The report is available online from www.dcaf.ch/Publications/Making-Intelligence-Accountable.

and its operation after a reasonable period by the PJCIS so as to demonstrate its ongoing value to security investigations. ASIO will also report on the value of the scheme, including the number of requests made for retained data, in its classified Annual Report to the Attorney-General and ministers.

Part 6 – Frequently asked questions

What are the arrangements for storing and accessing communications data?

In Australia communications data, where it is available, is stored and retained by the service provider. ASIO seeks to continue the arrangements under the TIA Act enabling access on national security grounds, clearly linked to ASIO's statutory functions, to communications data retained by service providers.

Does ASIO comprehensively monitor web surfing of all Australians?

The bill rules out the mandatory retention of web browsing histories from the data retention scheme. ASIO supports this position and is not seeking for providers to be required to retain web browsing histories, including in the form of histories of IP addresses or URLs visited. Where ASIO needs to collect the content a citizen's web browsing activity to pursue a defined security matter, ASIO seeks a warrant from the Attorney-General and the usual legislative thresholds, independent legal reviews, and oversight by the IGIS apply.

Does ASIO trawl Australia's communications data for security purposes?

ASIO only seeks communications data from service providers under the TIA Act where ASIO has grounds to conclude that it may have a nexus to a security matter. ASIO does not abuse the legislative provisions by requesting wholesale volumes of communications data from providers so as to trawl through it to identify individuals of potential concern. The concern expressed by some in the public domain that ASIO can, or does, monitor the communications of all Australians is unsupported.

The facts are that the IGIS reviews ASIO's requests for access to communications data, both historical data and prospective data, and in her most recent report to Parliament said that '[she] did not identify any concerns with ASIO's access to prospective and historic telecommunications data. My office's oversight of this particular technique decreased during this reporting period due primarily to changes in our inspection program and the high rate of compliance in this area.' [21]

Should ASIO need a warrant to seek telecommunications data?

In ASIO's view, the process to seek telecommunications data is already subject to stringent accountability mechanisms, including in ASIO's case independent oversight by the IGIS who has the powers akin to those of a standing royal commission. We believe these mechanisms are appropriate to detect and respond to

[21] For more information see 'ASIO access to telecommunications locational information or subscriber data' on pp.20-21 of *Inspector-General of Intelligence and Security Annual Report 2013-2014*. The IGIS annual report is available online from http://www.igis.gov.au.

any inappropriate use of the capability. For example, the IGIS would report to the Parliament on any abuse, overuse or misuse of telecommunications data by ASIO. ASIO's concern with implementing a warrant regime for data access is its impact on our operational response and agility: the significant bureaucratic overlay such a scheme would impose and the consequential delay in assessing and responding to emerging security threats before they are realised.

What are the checks and balances in the collection of information?

ASIO officers must collect information using the most effective means that are proportionate to the gravity of the threat and its likelihood. They do this within a legislative framework, acting under their authority delegated to them by the Director-General and in accordance with ASIO's code of conduct, internal policies and procedures. The Attorney-General's Guidelines state:[22]

> **Conduct of inquiries and investigations**
>
> 10.4 Information is to be obtained by ASIO in a lawful, timely and efficient way, and in accordance with the following:
>
> (a) any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence;
>
> (b) inquiries and investigations into individuals and groups should be undertaken:
>
> (i) using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions; and
>
> (ii) with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest;
>
> (c) the more intrusive the investigative technique, the higher the level of officer that should be required to approve its use;
>
> (d) wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and
>
> (e) where a threat is assessed as likely to develop quickly, a greater degree of intrusion may be justified.

These principles apply to ASIO's requests for access to communications data, and are reflected in ASIO's policies, procedures, and internal governance applying to investigative activities. Compliance with the guidelines is overseen by the IGIS. In her most recent annual report, the Inspector-General noted that '...ASIO has regard to the Attorney-General's Guidelines and is meeting the legislative requirement to only make requests for data in connection with the performance of its functions.'[23]

---

[22] The Attorney-General's Guidelines can be accessed online from ASIO's website via www.asio.gov.au/About-ASIO/Oversight-and-Accountability.html

[23] For more information see 'ASIO access to telecommunications locational information or subscriber data' on pp.20-21 of *Inspector-General of Intelligence and Security Annual Report 2013-2014*. The IGIS annual report is available online from the IGIS website via www.igis.gov.au.

What are the constraints on ASIO's handling of personal information?

A security intelligence agency that does not safeguard personal information about its citizens will ultimately fail in its statutory functions. ASIO takes very seriously its responsibility to protect and keep confidential any personal information it may hold about Australians, including persons under investigation as well as persons assisting ASIO to carry out its statutory responsibilities. Any dissemination of such information to other agencies is governed precisely by law.

The Attorney-General's Guidelines to ASIO direct that, in undertaking investigations, there should be as little intrusion into individual privacy as possible. ASIO is also required to protect personal information from unnecessary or unauthorised public disclosure. The Guidelines direct ASIO in how to treat personal information:[24]

> **13 Treatment of Personal Information**
>
> 13.1 ASIO shall only collect, use, handle or disclose personal information for purposes connected with its statutory functions.
>
> 13.2 The Director-General shall take all reasonable steps to ensure that personal information shall not be collected, used, handled or disclosed by ASIO unless that collection, use, handling or disclosure is reasonably necessary for the performance of its statutory functions (or as otherwise authorised, or required, by law).
>
> 13.3 The Director-General shall ensure that all reasonable steps are taken to ensure that personal information held, used or disclosed by ASIO is accurate and not misleading.
>
> 13.4 Appropriate records shall be kept of all requests made by ASIO for access to personal information and all personal information received in response to such requests. Such records shall be open to inspection by the Inspector-General of Intelligence and Security.
>
> 13.5 Appropriate records shall be kept of all communication by ASIO of personal information for purposes relevant to security or as otherwise authorised. Such records shall be open to inspection by the Inspector-General of Intelligence and Security.
>
> 13.6 The Director-General shall ensure that all personal information collected or held by ASIO is protected by reasonable security measures against loss and unauthorised access, use or modification.

While ASIO is exempt from the operation of the *Privacy Act 1988* (Privacy Act), the Attorney-General's Guidelines are consistent with the principles underpinning the operation of the Privacy Act, to the extent that is possible consistent with the need for an effective security intelligence capability. The need to foster human rights protection and protect Australia from national security threats is one of the underlying principles of ASIO's internal accountability framework.

[24] The Attorney-General's Guidelines can be accessed online from ASIO's website via www.asio.gov.au/About-ASIO/Oversight-and-Accountability.html

What does ASIO do to implement the Attorney-General's Guidelines on the treatment of personal information?

ASIO systems and databases where communications data is stored are subject to a security model and accessible only to officers with a need for such access to do their jobs. This means only officers directly involved in assessments, analysis, operations, or responsible for the maintenance of the systems, can access communications data. All access may be audited to identify unauthorised or inappropriate access.