Australian Government
Australian Security Intelligence Organisation

ASIO Submission to the Senate inquiry into a comprehensive revision of the *Telecommunications (Interception and Access) Act 1979*

February 2014

www.asio.gov.au

ASIO Submission to the Senate inquiry into a comprehensive revision of the Telecommunications (Interception and Access) Act 1979

Table of contents

Part 1 – Introduction

ASIO welcomes the opportunity to assist the Legal and Constitutional Affairs References Committee in its deliberations as to whether a comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) is required. It is ASIO's view that some revision is required but that the principles underlying the 1979 Act should remain in place.

In line with the inquiry's Terms of Reference this submission addresses the recommendations made by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its *Report of the inquiry into potential reforms of Australia's national security legislation* and the Australian Law Reform Commission's (ALRC) report, *For information: Australian privacy law and practice*. This submission reflects the views of ASIO only. The Government has made no decisions in relation to the comprehensive revision of the TIA Act, nor in relation to the recommendations contained in the PJCIS report.

To provide context, this submission will seek to explain the value and use of telecommunications interception and telecommunications data to ASIO activities. Both capabilities have contributed to identifying and countering serious threats to security, including threats to Australian lives. It will also seek to dispel a number of misconceptions which have surfaced in respect of ASIO's and law enforcement access to and use of telecommunications data, particularly in the wake of the leaks by former United States National Security Agency contractor, Edward Snowden.

This submission is divided into parts as follows:

Part 2—Executive summary

There is a significant difference between telecommunications interception and the collection and analysis of telecommunications data. The first relates to the actual essence or content of a communication (the conversation, email etc). The second is specific information to ensure the communication takes place or relates to those who are communicating. To use a basic analogy, content is the letter and telecommunications data the envelope.

Information derived from telecommunications systems plays a central role in many national security and law enforcement investigations. It represents a key source of intelligence to prevent harm. In the modern age the ability to save lives and protect our national security would be severely limited without these tools. For example, intelligence from telecommunications interception under warrant and telecommunications data has been critical to the identification and disruption of all the planned mass casualty terrorist attacks in Australia since 2001.

The majority of the Australian community expect ASIO to use these tools where real harm is in prospect and needs to be prevented. However, there are significant misconceptions in the public discussion of their use, including the extent to which they are used for national security and law enforcement purposes. The governance arrangements in place mean telecommunications interception or data is only sought by ASIO where it is required to resolve a security matter and is done so minimally.

ASIO does not have the resources, the need, or the inclination to undertake the large-scale mass gathering of telecommunications data often alluded to in the public sphere. 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 telecommunications 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 telecommunications interception of content under warrant where needed.

ASIO accepts that privacy requirements need to 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, ASIO proactively informs the Inspector-General of Intelligence and Security (IGIS) who reports them to the Parliament in her annual report. ASIO is not seeking to weaken such accountability.

Some legislative modernisation, however, is needed. Without it, developments in the telecommunications environment will 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 telecommunications 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.

Part 3—Security intelligence in Australia

Security and intelligence agencies perform an important function in modern societies. The Australian Government uses intelligence to pursue and protect our national interests and to inform its decision-making. Security intelligence is vital to protecting Australia, its interests and its people.

ASIO's role as Australia's security service is anticipatory and protective in nature: we are expected to detect and stop terrorist attacks and to thwart spies. ASIO's roles and responsibilities are precisely defined by the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). The ASIO Act specifies ASIO's remit as 'security', which it defines as the protection of Australia and Australians from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence systems, foreign interference and serious threats to Australia's territorial and border integrity.

This security intelligence mandate is directed at protecting Australia's sovereignty, democratic institutions and freedoms, and citizens from security threats. It is anticipatory in nature: ASIO is required to collect intelligence so that it can assess and predict threats before such threats become reality; that is, ASIO's role is to predict the bomb attack and enable preventative action, not to investigate and prosecute the perpetrators after the fact. The threats are concrete: Australia is a terrorist target, and foreign intelligence services actively engage in espionage and influence activities against Australia. Certain threats to national security—including to the lives of Australians—are grave enough to require ASIO to exercise special powers in detecting them: in the majority of instances, such threats can only be assessed and mitigated by the use of such powers. At the same time, ASIO is acutely aware of the complementary priorities of protecting individual rights and minimising intrusion.

The ASIO Act places a special responsibility on the Director-General of Security to keep the Organisation free from any influences or considerations–including political considerations–that are not relevant to its functions. The ASIO Act prevents ASIO from undertaking any activity that would limit the right of people to engage in lawful advocacy, protest or dissent.

In fulfilling its obligations to protect Australia, its people and its interests, ASIO:

- collects intelligence, including via human sources and technical operations;
- assesses intelligence and provides advice to the Australian Government on security matters;
- identifies and investigates threats to security, such as politically motivated violence and espionage, as specifically defined in the ASIO Act;
- maintains a national counter-terrorism capability;
- provides protective security advice; and

- provides security assessments.

In carrying out its work, ASIO observes guidelines provided by the Attorney-General in accordance with the ASIO Act. The *Attorney-General's guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* are publicly available from ASIO's website.[1]

The guidelines require ASIO to identify previously unknown persons, groups and entities that may present a risk to security. ASIO's goal is to provide advice to inform the risk management of security matters. The earlier ASIO can provide such advice to enable preventative action, the greater the reduction in risk to Australia, its interests and its people.

For ASIO to be effective it has no option but to intrude into the privacy of a very small number of people relative to the overall population. A certain level of intrusion is inevitable in almost all security investigations, exacerbated by our adversaries actively disguising or hiding their intentions and activities. For example, ASIO is aware of foreign cyber actors calibrating their operations on Australia's telecommunications infrastructure to exploit limitations in Australia's legislative framework and technical capabilities—they actively seek to operate in ways and spaces to make it more difficult for ASIO to detect and defeat their activities.

ASIO is also 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 (see Box 1, 'What does "relevant or prejudicial to security" mean', below). Security inquiries more often than not determine that a person is actually not a security threat.

With this in mind, the guidelines require ASIO to observe the principle of proportionality, which means the Organisation must use the least intrusive investigative means to collect information, commensurate with the level of threat and the likelihood of it eventuating. This means the most intrusive techniques are reserved for security matters where ASIO is satisfied people or groups are capable of harming Australia or threatening the lives and safety of Australians. This principle of proportionality is embodied in ASIO's culture, training and policies, and is a part of the day-to-day decisions individual ASIO officers make.

Authorisation for the most intrusive activities by ASIO, including telecommunications interception under warrant, is not sought until the Organisation is satisfied (and has established a reasonable suspicion in the case of TI) that the individual or group is engaged in activities prejudicial to security (a significantly higher test than 'relevant'). Authorisation is not sought without consideration to the proportionality of the intrusive activity compared to the likely harm if the activities that are prejudicial to security are allowed to proceed unchecked.

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

What does relevant or prejudicial to security mean?

The Attorney-General's guidelines[2] in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)include the following definitions:

Information obtained by ASIO is relevant to security where it may assist ASIO in determining whether:

(a) there is a connection or possible connection between a subject and activities relevant to security, irrespective of when such activities have occurred or may occur;

(b) the activities of a subject are not relevant to security; or

(c) a person, group or entity other than the subject has a connection or possible connection to activities relevant to security.

Activities relevant to security means not only physical acts of the sort specified in the definition of security, but also includes the acts of conspiring, planning, organising, counselling, advising, financing, or otherwise advocating or encouraging the doing of those things.

Activities prejudicial to security means activities that are relevant to security and which can reasonably be considered capable of causing damage or harm to Australia, the Australian people, or Australian interests.

Accountability

Australia's approach to intelligence activities has a clear focus on lawfulness, proportionality, and accountability, achieved through the four key strands of:

- **Legislation** governing Australia's intelligence community and weighing of collective security rights and the rights of citizens, including to privacy.
- **Parliamentary oversight** of intelligence activities, in particular through the Parliamentary Joint Committee on Intelligence and Security.
- **Ministerial accountability** ensuring clear lines of accountability, including through ministerial guidelines on intelligence agencies (such as in relation to privacy).
- **Independent oversight** by the Inspector-General of Intelligence and Security (IGIS).

The IGIS has a key role in providing assurance to Government and the community in relation to ASIO's activities. The Inspector-General is an independent statutory officeholder empowered to review the legality, propriety, and human rights aspects of intelligence activities, as well as compliance with ministerial guidelines, and report directly to ministers. The Inspector-General conducts ongoing inspections of ASIO's activities—particularly its operational activities—and initiates own motion inquiries or when referred by ministers. The Office of the IGIS has access to ASIO's records, can interview ASIO's staff, and enter ASIO's premises. The IGIS reports on the outcomes of these inspections and inquiries to the Attorney-General, other ministers as appropriate, and Parliament.

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

The oversight and accountability mechanisms applying to ASIO's activities include the following elements:

Legislation, for example:

- *Australian Security Intelligence Organisation Act 1979*
- *Telecommunications (Interception and Access) Act 1979*
- *Archives Act 1983*
- *Inspector-General of Intelligence and Security Act 1986*
- *Financial Management and Accountability Act 1997*
- *Intelligence Services Act 2001*
- *Independent National Security Legislation Monitor Act 2010*
- *Work Health and Safety Act 2012*
- *Public Interest Disclosure Act 2013*
- *Public Governance, Performance and Accountability Act 2013* (from 1 July 2014)

Parliamentary oversight

- ASIO's annual report to the Parliament.
- Parliamentary Joint Committee on Intelligence and Security.
- Briefings of the Leader of the Opposition.
- Senate estimates.
- Portfolio Budget Statement.

Ministerial accountability

- Attorney-General's Guidelines on security intelligence.
- ASIO's classified Annual Report to the Attorney-General and ministers.
- Briefings to the National Security Committee of Cabinet.
- Approval by the Attorney-General to use warrant powers (and a judicial officer in the case of questioning and detention powers).
- Approval by the Attorney-General for ASIO to liaise with international partners.
- Reporting to the Attorney-General on the value and intelligence obtained from each warrant.
- Regular advice and reporting to the Attorney-General.

Independent oversight

- Inspector-General of Intelligence and Security.
- Independent National Security Legislation Monitor.
- Australian National Audit Office.
- Independent Reviewer of Security Assessments.
- Security Appeals Division of the Administrative Appeals Tribunal.
- Judicial review.
- Review by the Attorney-General's Department of each case ASIO submits for a warrant to ensure it meets the legislative test.

These elements are designed to be as public as possible, consistent with the requirements of national security. For example:

- ASIO provides the Attorney-General and ministers with a national security classified annual report detailing ASIO's outcomes and performance, and the Attorney-General subsequently tables an unclassified version in Parliament,
- The IGIS provides national security classified advice on outcomes of inspections and inquiries to ASIO and the Attorney-General. The Inspector-General also provides an annual report of these activities to Parliament.
- The Parliamentary Joint Committee on Intelligence and Security conducts an annual review of administration and expenditure of intelligence agencies. The committee has access to national security classified material and briefings to inform its report to the Parliament.
- While the detailed breakdown of ASIO's expenditure is not publicly available, aggregate information appears in the Portfolio Budget Statement, and financial statements audited by the Australian National Audit Office are published in ASIO's annual report to Parliament.

The Director-General of Security also makes speeches, attends community forums, and ASIO engages with the media as appropriate.

Some elements of ASIO's accountability mechanisms are by necessity maintained in private, such as ASIO's reports to the Attorney-General on the value and intelligence from each warrant, briefings to Cabinet, and briefings to the Leader of the Opposition.

This balance of public and private accountability measures is right for an intelligence organisation needing to maintain secrecy of its sources, methods, and operational capabilities so as to protect Australians from harm.

Community attitudes to national security

There is another balancing of principles in relation to ASIO's work and that is between individual human rights such as privacy and the collective community right to a secure and safe environment. In ASIO's view, this balance is currently about right. Nevertheless, it always has been—and it is appropriate it always will be—the subject of ongoing debate. There are indications from small polls that the Australian community understands the need to balance privacy concerns with the need to protect the community, and also that the community is not as concerned about government surveillance as might be portrayed in the public debate.

The Lowy Institute for International Policy sought people's views on the Australian Government's measures to combat terrorism, in its March 2013 survey of 1002 Australians.[3] 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 government leans too much toward protecting the rights of citizens over fighting terrorism'. Nineteen per cent believed the opposite.

[3] The Lowy Institute's poll is available from www.lowyinstitute.org/publications/lowy-institute-poll-2013.

The Office of the Australian Information Commissioner sought people's views on the biggest privacy risks, in its June–July 2013 survey of 1000 Australians for its *Community attitudes to privacy* report[4]. 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.

Part 4—ASIO's use of telecommunications content

ASIO's use of telecommunications systems as a source of intelligence can be divided into two distinct parts:

- **Content** collection and analysis: the lawful interception and analysis of all traffic sent or received by a particular service or device. This includes the capture of all conversations, documents (including email), applications and media. A warrant is required for this intrusive collection of content.
- **Telecommunications data** collection and analysis: access to and the analysis of specific data collected and stored by a telecommunications carrier, carriage service or internet service provider for its normal business purposes. Given the lesser level of intrusion, access to this data has never been subject to warrant, nor should it be. But it is nevertheless regulated by internal processes and subject to external review to ensure it is used only when necessary to carry out ASIO's functions.

This part outlines ASIO's use of telecommunications content. ASIO's use of telecommunications data is discussed in Part 5.

What is the value of telecommunications interception to ASIO?

In ASIO's view, the use, value and necessary intrusion of the lawful interception of telecommunications content to prevent harm to Australia is well understood by the Australian public.

Telecommunications interception of content is a key tool in preventing harm because people engaged in activities of security concern must communicate to progress their intentions. The

[4] 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.

availability, convenience and variety of telecommunications services mean such services are almost inevitably used for this purpose. Therefore, access to telecommunications content provides essential details of activities of security concern and enables ASIO to provide advice and take action to protect Australia.

The most effective way ASIO can illustrate how TI has contributed to security intelligence investigations is to provide concrete case studies.

Case studies: countering terrorism

- Telecommunications content intercepted by ASIO has helped prevent mass casualty terrorist attacks in Australia. It was crucial, for example, in the NSW prosecutions connected with terrorist plot known as Operation Pendennis led by Abdul Nacer Benbrika. The telecommunications content included intercepted conversations, SMS messages and internet activity. It showed the ideology, intentions and plans of the men, as well as the activities they engaged in to progress their plot. The material, uniquely collected by ASIO, formed a substantial part of the prosecution case which resulted in five men being found guilty by a jury (receiving prison sentences ranging from 23 years to 28 years) and the remaining four pleading guilty to lesser terrorism offences.
- Interception of telecommunications content under warrant assists ASIO day-to-day to monitor the activities of individuals and groups plotting to use violence to achieve a political objective in Australia or overseas. There have been many cases aside from Operation Pendennis where preventative measures have been implemented as a result of the collection and analysis of telecommunications content and deflected individuals from pursuing their extremist intent. Not all of these have lead to prosecution or are detailed in the public domain.
- Telecommunications content lawfully intercepted by ASIO also formed a critical part of the evidence against Belal Khazaal on terrorism charges relating to his activity in September 2003. The material collected linked Khazaal to possessing a book on how to engage in violent jihad. Khazaal was found guilty by a jury (confirmed by the High Court of Australia) and received a prison sentence of 12 years.

Frequently asked questions

How often are warrant powers used?

Justice Hope noted in 1984 that 'fewer telephone interceptions and other warrant operations are carried out than is often popularly supposed'.[5] The same can be said today. ASIO does not engage in wholesale interception of telecommunications content across the whole community as is sometimes intimated in the public arena. As stated earlier in this submission, 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. Of this minority only a small proportion may be suspected of seeking to do actual harm to Australia, its people or its interests.

[5] Royal Commission on Australia's Security and Intelligence Agencies, *Report on the Australian Security Intelligence Organization*, December 1984. Paragraph 6.60.

It is this small proportion who may be subject to more intrusive investigation, including telecommunications interception of content under warrant where needed.

ASIO's classified annual report details to the Attorney-General and other ministers the number of warrants sought and issued. TI is used in those serious security matters where ASIO is satisfied and has established a reasonable suspicion that the individual or group is engaged in activities prejudicial to security. The number of ASIO telecommunications interception warrants includes individuals engaged in the range of security activities defined in the ASIO Act—predominantly in the areas of politically motivated violence, espionage, and foreign interference—as well as warranted interception at the request of the ministers for Foreign Affairs and Defence to collect foreign intelligence in Australia. Warrants only remain in force for a maximum of six months and the figures reported in ASIO's classified annual report include warrants renewed against the same person.

Does ASIO retain information that is not relevant to security?

Telecommunications interception of content under warrant is intrusive and, while efforts are made to filter out obviously non-security related product, it remains inevitable that some personal information and communications will be accessible to ASIO. However, only information which has a relevance to security will normally be retained for future reference by the Organisation in its databases.

The use of the word 'normally' needs explanation. In investigations where intercept product has the potential to be used in a future prosecution case, ASIO will retain all collected product from the interception to meet evidentiary and discovery requirements. However, only product considered relevant to security will have been processed and made accessible to ASIO investigators.

Part 5—ASIO's use of telecommunications data

The definition and value of telecommunications data is often misunderstood or incorrectly represented. Telecommunications data falls into two categories (see Table 1).

Category 1: Information that allows a communication to occur.	Examples: • the internet identifier (information that uniquely identifies a person on the internet) assigned to the user by the provider—for example, Internet Protocol (IP) addresses or an IP address and port number • for a telephony service: the number called or texted • the service identifier used to send a communication—for example, the user's email address, phone number or VoIP number (internet telephone number) • the time and date of a communication • general location information—for example mobile telephone cell tower • the duration of the communication
Category 2: Information about the parties to the communications and information about the person who owns or uses the service.	Examples: • the name and address of the customer • the postal and/or billing addresses of the customer (if different) • the contact details, mobile telephone number, email address and landline phone number of the customer • the same information on the recipient party if known by the service provider.

Table 1: Categories of telecommunications data

As Table 1 shows, telecommunications data is a broad label for a variety of elements, which vary depending on the business needs of each carrier. In most cases, it comprises the name and address of the owner of a specific service, the numbers or service identifiers of other services contacted by this service, the time and date, the duration and the cost of each communication. For a mobile service, the data can also include the location of a handset, which can range substantially in specificity.

What is the value of telecommunications data to ASIO?

The analysis of telecommunications data can provide important information to assist in the identification of a person of security concern, including that person's telecommunications activities or contacts within a defined time period. The analysis of this telecommunications data

reduces the need to undertake more intrusive and costly methods of investigation to determine whether an individual is indeed likely to be of potential relevance to security or engaged in activities prejudicial to security. Determining identity is key and ASIO relies on accessing telecommunications data to identify the subscriber to specific services of interest.

Case study examples can illustrate the value of telecommunications data in dealing with security intelligence leads and taking action to prevent harm.

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

- Telecommunications 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.

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

- An intelligence agency overseas provided ASIO with an Australian telephone number, which had been found during intelligence operations that disrupted an active terrorist cell. 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 data. An analysis of this data showed the individual had dialled a range of overseas numbers known to be linked to individuals engaged in extremist activity. The analysis also showed the individual was in regular contact with a number of individuals in Australia known to espouse extremist views.
- This investigation 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.

To obtain the same information via other means would be significantly more expensive and would require much higher levels of intrusion into a person's private life. The analysis of telecommunications data is a key component of almost all priority security investigations and consistently proves to be an invaluable intelligence capability, including to help eliminate individuals from security concern.

The experience of ASIO's partners is similar. For example, the then Director-General of MI5 was quoted by the UK Parliament's Intelligence and Security Committee in its February 2013 report, *Access to communications data by the intelligence and security agencies*, as saying:

> …access to communications data of one sort or another is very important indeed. It's part of the backbone of the way in which we would approach investigations. I think I would be accurate in saying there are no significant investigations that we undertake across the service that don't use communications data because of its ability to tell you the who and the when and the where of your target's activities. (p.9)

The committee went on to find that telecommunications data was central to the work of UK intelligence agencies, was particularly useful in the early stages of investigations and was the least intrusive way of determining whether individuals were of relevance to security (p.10). [6]

In the context of countering espionage and foreign interference, access to telecommunications data enables ASIO to securely identify, reliably assess and effectively counter the harm from clandestine or deceptive activity by foreign states against Australian interests. Telecommunications data provides unique insights to identify individual associations and connections vital to resolving issues that can emerge as security issues years after the event. The inability to access telecommunications data would severely affect ASIO's ability to investigate and counter espionage and interference activities by foreign states with strategic intent to harm Australia's national interest.

Frequently asked questions

What are the arrangements for storing and accessing telecommunications data?

In Australia telecommunications 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, and a highly targeted basis, to the telecommunications data that is normally retained by service providers for their telecommunications and business purposes.

Does ASIO comprehensively monitor web surfing of all Australians?

ASIO is not seeking for telecommunications service providers to retain web surfing data in the form of histories of sites or URLs visited. ASIO regards web browsing activities as requiring a higher degree of privacy protection than the telecommunications data outlined above in Table 1. Where ASIO needs to be informed for national security purposes of a person's web browsing activity ASIO would seek a specific warrant from the Attorney-General if the threshold is met.

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

ASIO does not request wholesale volumes of telecommunications data from telecommunications providers so as to trawl through it to identify individuals of potential concern. The concern expressed by some in the public domain that ASIO monitors the web browsing of all Australians is unsupported. ASIO will only seek and receive telecommunications data from the service

[6] The committee's report is available online from its website via http://isc.independent.gov.uk/committee-reports/special-reports.

provider under the TIA Act where ASIO has grounds to conclude the data may have a nexus to a security investigation.

For example, ASIO often relies on the analysis of telecommunications 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 data does not include, and has never included, the content of any communication to or from a specific service, nor is ASIO seeking to change the distinction under which content may be sought or collected under warrant. ASIO seeks access to content for security intelligence purposes only when there are indications the person using the service is likely to be engaged in activities prejudicial to security or the service is likely to be used for purposes prejudicial to security.

ASIO requires different levels of approval for requesting telecommunications data:

- **Historical** telecommunications data can only be requested from a service provider by an ASIO officer authorised by the Director-General.
- **Prospective** telecommunications data requires a higher level of approval because the request is for the service providers to retain telecommunications data relating to specified services or individuals who are the subject of security investigation. The requests to the service providers are authorised by a Senior Executive Service Band 2 officer or higher. Compared to requests for historical telecommunications data, a higher approval level is required because the request is seeking access to data that is yet to be generated.

For requests for either historical or prospective telecommunications data, 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.

This process, including the examination of records, is the subject of oversight by the IGIS. The *IGIS annual report 2012–13* found overall 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).[7]

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

[7] The IGIS annual report is available online from http://www.igis.gov.au.

appropriate to detect and respond to 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.

Part 6—Accountability for ASIO's use of telecommunications content and data

As outlined in Part 3 of this submission, ASIO operates under multiple layers of oversight and accountability, including independent external scrutiny, and these all apply to ASIO's use of telecommunications interception and telecommunications data.

In relation to ASIO's use of telecommunications interception and data specifically, in his 2013 Sir Zelman Cowen Oration to the Australian Institute of International Affairs the Director-General of Security noted six principles articulated by Sir David Omand, a former Chairman of Britain's Joint Intelligence Committee, for ethical and effective surveillance and interception:

- 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
- Recourse to secret intelligence must be a last resort.[8]

These concepts are found within the accountability measures governing ASIO's use of telecommunications interception and telecommunications data.

- ASIO has procedures in place to ensure the people of ASIO understand our legislation, internal policies and procedures, and approach and accountability mechanisms.
- ASIO's methods are required to be proportionate—and are.
- ASIO has detailed authorisation processes for the use of telecommunications interception, with the Attorney-General needing to be personally satisfied that each case presented by ASIO meets the test set out by Parliament.
- ASIO's telecommunications interception and data activities are subject to regular review by the Inspector-General of Intelligence and Security, who reports on the small number of occasions where an error is made to the Parliament.

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

- ASIO's security intelligence activities are prioritised on the basis of greatest or most immediate threat or harm. ASIO does not have the resources to engage in frivolous, wasteful, or irrelevant eavesdropping of the community's private conversations.
- The ASIO Act regulates the sharing of security intelligence and ASIO has measures in place to secure and protect information it collects.

In ASIO's view, the internal accountability measures are appropriate, as is their implementation. It is essential this accountability framework continues to provide assurance to Government and the public of the legality and propriety of agency access to data and interception, while not impeding agile operational decision-making in the prevention of harm to Australia from national security threats and serious crime. ASIO believes the appropriate balance is present in the national security space, through ministerial accountability and oversight by the Inspector-General.

Frequently asked questions

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

As mentioned earlier in the submission, 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:[9]

> **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 interception activities, as well as to its requests for access to telecommunications data, and are reflected in ASIO's policies, procedures, and internal

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

governance applying to investigative activities. Compliance with the guidelines is overseen by the Inspector-General of Intelligence and Security.

What are the additional checks and balances in relation to warrants?

The Attorney-General, informed by the Director-General of Security, is the final decision point for deciding whether an intelligence case meets the relevant legislative test and for approving or declining ASIO's requests to use intrusive warrant powers.

In addition, ASIO's business practices in the use of warrant powers have a series of checks and balances designed into them. These appear at all stages, including as the investigation progresses, prior to a warrant being submitted to the Attorney-General and after the request for the warrant is approved.

- Prior to the requests for warrants being approved, they undergo internal review by ASIO's Office of Legal Counsel, and external review by the Attorney-General's Department. The Director-General must also be satisfied there is a security intelligence case before formally submitting the request to the Attorney-General.
- After warrants are issued, the warranted activity is subject to internal review mechanisms as well as external inspection and review by the Inspector-General of Intelligence and Security (see *How are ASIO's interception activities independently reviewed?* below*).*
- After the warrant period concludes ASIO provides a report to the Attorney-General on the value of the intelligence collected.

How are ASIO's interception activities independently reviewed?

Interception of communications is an intrusion into individual privacy. This is why all interception activities carried out by ASIO are conducted in accordance with Australian law and are fully accountable through ministerial oversight.

In relation to ASIO's interception activities there is also independent monitoring by the IGIS. In the small number of cases where interception errors occur, typically ASIO self-identifies and reports these to the IGIS and, in concert with the telecommunications carriers, takes remedial action. These cases are all regularly reported in the annual report provided by the IGIS to the Parliament. In 2012–13 the IGIS noted a relatively small number of cases either by ASIO or the relevant service provider which had been proactively advised to the IGIS by ASIO. The *IGIS annual report 2012–13* notes the handful of errors '…could be attributed to the often dynamic nature of modern telecommunications, or to human error' by ASIO or the carriers (p.18).[10]

ASIO is required to report to the Attorney-General on the intelligence value of each warrant. In 2012–13 the IGIS identified no instances where such a report was not provided to the Attorney-General.

[10] The IGIS annual report is available online from http://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 indeed 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 it 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:[11]

> **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. This is one of the underlying principles of ASIO's internal accountability framework.

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

ASIO TI systems, and databases where TI product is stored, are strictly compartmentalised and accessible only to officers with a need for such access to do their jobs. This means only officers directly involved in an investigation, or responsible for the maintenance of the intercept and

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

storage systems, can access product collected as part of a warranted operation connected with a particular investigation. All access may be audited to identify unauthorised or inappropriate access.

Part 7—The need for legislative modernisation

ASIO strongly supports the basic right of individual Australians to privacy, but commensurate with the Government's first duty to protect the national interest and the lives and safety of Australian citizens.

ASIO's role and functions are provided for in law by the Parliament and in this way recognised as vital for Australia's security. ASIO intrudes into the lives of only a minute proportion of the community and only when necessary to protect the community and nation as a whole. Telecommunications systems represent a key source of intelligence enabling ASIO to predict and help prevent harm. Its importance as a tool of national security cannot be understated. ASIO's ability to protect Australia from security intelligence threats is at risk because of limitations in Australia's current TI legislative regime.

The ALRC and PJCIS reports recognise the need for ASIO and law enforcement agencies to continue to engage in telecommunications interception. While interception agencies, with the assistance of carriers, are attempting to keep up with technology, business and social change, the prospect of 'going dark' and losing the ability to collect and understand this important source of intelligence continues to increase.

Over the years, the TIA Act has become cumbersome, outmoded, and open to conflicting interpretations, particularly in regard to changes in technology, business and consumer practices. It is not meeting the need to protect national security interests and the lives and safety of Australians; it is not meeting the needs of interception agencies. ASIO and other interception agencies are seeking to establish a regime that is sufficiently robust and technologically neutral so as not to require revision with each new technological or business development.

What is the basis for the current legislative regime?

The TIA Act and the *Telecommunications Act 1997* regulate interception and access to telecommunications 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.

When the current TIA Act was first drafted, there was one national carrier. There was no World Wide Web, no widespread adoption of the internet; services were restricted to copper-wire infrastructure, and communications were to and from fixed locations. The vast majority of telecommunications traffic was unencrypted voice, though fax services were starting to be introduced. A subject of ASIO investigation had access to one fixed phone at his or her residence, potentially access to a fixed phone at his or her place of employment, and access to public phone boxes.

The current legislative framework was developed in a very different era, where technology, industry and consumer behaviour were dramatically different. The fundamental assumptions underlying the current legislative regime include the following:

- Telecommunications providers had clear obligations to assist agencies or were able to intercept communications on their behalf.
- Telecommunications providers were based in Australia and willing to work securely with agencies.
- The service provider held the telecommunications data critical for agency investigations.
- It was easy to determine which provider was being used by a person of interest.
- It was easy to determine the communications service being used by a person of interest.
- Communications were not encrypted or would be provided to agencies in a readable, viewable or un-encrypted form.
- The technical means needed to intercept services could easily be implemented.

Many of these assumptions no longer hold.

How is the telecommunications environment changing?

Today there are numerous telecommunications carriers and even more numerous carriage and internet service providers. Today's telecommunication services are international and the network infrastructure and service are located overseas. Most citizens use several communication services: fixed line, mobile phone, mobile broadband, free wi-fi. The internet is accessible from just about anywhere and offers a range of services including email, VoIP, social media and file sharing, many requiring no or little identification to use and delivered by ancillary service providers.

The amount of information sent to and received by communication devices continues to increase exponentially. The content of telecommunications includes voice, music, film, documents and books. Information sent across the system can and often is encrypted by the carrier, the carriage service provider, the customer, or a combination of all three.

The business practices of the telecommunications industry are also changing, driven by the desire to gain market share and operate around the globe, as well as to reduce cost and increase profit. The business practice of charging for the time taken for the communication transaction is changing to a practice of charging for the data download and upload across the service—that is if they charge by individual transactions at all: there has also been a trend of providers moving to volume-based monthly plans, including unlimited calls. In essence, telecommunications providers only need to know in the moment where to send a communication and to whom it should be sent; they only retain the details of the amount of data sent for their billing purposes. The current and future absence of meaningful telecommunications data will have a significant detrimental impact on almost every ASIO investigation to the extent that we will not be able to effectively acquire and assess telecommunications information. ASIO would be rightly open to accusation it could not effectively undertake our role in protecting Australia and its people.

These changes are becoming far more significant in the security environment following the leaks of former NSA contractor Edward Snowden. Since the Snowden leaks, public reporting suggests the level of encryption on the internet has increased substantially.[12] 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.

What do these trends mean for security intelligence capability?

Changes to the telecommunications environment have meant our ability to intercept communications under the current regime is under significant threat. Unless the telecommunications interception regime modernises and unless we develop new capabilities, law enforcement and security agencies face the prospect of progressively continuing to lose critical intelligence and evidentiary collection capabilities—the 'going dark' problem.

For example, the practice of internet service providers automatically allocating and reallocating temporary Internet addresses (that is, the IP addresses and port numbers that the network protocols use to enable communication between computers) to their customers has flow-on effects for security intelligence investigations. Determining who sent or received a specific communication, or who accessed a certain website, can be a significant challenge.

Nearly every ASIO investigation, including those into emerging threats, requires access to telecommunications data of some form. This is the reason ASIO has been seeking a regime, along the lines of the one in operation in the European Union, whereby companies providing telecommunications services are responsible for retaining telecommunications data for a set period of time. This would ensure that relevant elements of telecommunications data vitally important for ASIO to investigate threats to national security is available for a clearly defined period of time.

Increasingly, interception agencies are no longer dealing with the certainty of collection, but the possibility of collection. Changes in the telecommunications environment are affecting the ability of agencies to:

- **reliably identify communicants** of interest and associate them with telecommunications services—this is a consequence of anonymous access to telecommunications services and impediments to agency access to subscriber 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.

[12] For example see www.sinefa.com/encrypted-traffic-grows-post-edward-snowden-nsa-leak

The PJCIS and ALRC recognise in their reports the need for legislative revision—as we see it modernisation—including to ensure national security and law enforcement agencies have appropriate access to telecommunications content and data.

This situation is not unique to Australia. Internationally, the need to address these challenges in order to ensure national security and public safety has been considered, for example by the following:

- US congressional hearings in 2011 (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) during which the FBI detailed the challenges it faces[13].
- the UK Parliament in 2013 (Intelligence and Security Committee report on *Access to communications data by the intelligence and security agencies*)[14]; and
- statements by the President of the United States in the wake of the Snowden leaks[15].

Outside of government there is also a growing recognition of the need to respond to the changing environment. For example, in the International Chamber of Commerce (ICC) has issued policy statements in 2010 and 2012 titles, respectively, *Global business recommendations and best practices for lawful interception requirements* and *Using mutual legal assistance treaties (MLATs) to improve cross-border lawful intercept procedures*. The ICC policy statements acknowledge the need to preserve investigative capabilities in an Internet Protocol-enabled world and makes a number of recommendations, from a business and commerce perspective, to balance the benefits and costs of interception regulation[16].

[13] See FBI evidence and the hearing transcript for more detail. Available online from: 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.

[14] The committee's report is available online from its website via: isc.independent.gov.uk/committee-reports/special-reports.

[15] 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.

[16] The policy statements are available online from the International Chamber of Commerce's website: www.iccwbo.org http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2010/ICC-policy-statement-on-Global-business-recommendations-and-best-practices-for-lawful-intercept-requirements/ ; and http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/mlat/ .

Part 8—What are the required elements of legislative modernisation?

This section of the submission describes ASIO's overall view on how the legislation needs to be modernised. ASIO agrees with the overall recommendation by the PJCIS that the TIA Act needs to be comprehensively revised (Recommendation 18), and with the majority of the specific changes recommended by the PJCIS and ALRC. ASIO's detailed comments in relation to the PJCIS and ALRC recommendations can be found in part 9 of this submission.

In summary, it is ASIO's view the telecommunications legislative regime needs to be modernised so as to:

1) enable national security and law enforcement agencies to continue to access telecommunications data from providers and undertake telecommunications interception;
2) continue to provide appropriate accountability and oversight, including in ASIO's case through the Attorney-General and the IGIS;
3) be overall technology-neutral;
4) require data retention by telecommunications providers;
5) confirm who is obligated to provide interception capability and other assistance, having regard to the dramatically changed telecommunications environment and noting the following:
   (a) every telecommunications player who provides services to the public and carries communications should be subject to that obligation; and
   (b) there should be clear articulation of the nature of those obligations, including the distinction between telecommunications content and data;
6) set technology-neutral standards for interception capability and other assistance, dealing with capability requirements, delivery of information in a useable form and security standards.

These elements are largely consistent with the recommendations made by the PJCIS and ALRC. Aside from the first point which is the subject of Parts 4 and 5 of this submission, each of these elements is dealt with under a heading below. The main area of contention appears to rest in the area of access to, use of, and retention of telecommunications data; ASIO's reasons for advocating this approach and its benefits are detailed below.

Accountability and oversight

Accountability and oversight must remain a critical component of any redrafted legislation. It is essential that this accountability framework continue to provide assurance to Government and the public of the legality and propriety of agency access to data and interception, while not impeding agile operational decision-making in the prevention of harm to Australia from national security threats and serious crime. Current oversight and accountability processes are suited to any new regime. Care must be taken to avoid creating an unnecessarily cumbersome and inefficient system of oversight.

Technology-neutral legislation, including attribute interception

In ASIO's view, it is necessary to decouple the ability to seek interception from current technologies, such as a phone number. This needs to happen to ensure that agencies can respond with agility and flexibility to future threats and technical developments. This is not intended to reduce accountability; rather, it ensures legislation keeps pace with the activities and methods required for effective investigation of threats to national security and of serious crime. Attribute interception, if broadly defined within a revised TIA Act, would provide for unforeseen future technological and business changes within the telecommunications industry without having to reinterpret or constantly revise the Act. For example, attribute interception would enable agencies to seek interception based on a unique identifier for a telecommunications service (such as a user name) even if such identifiers were not envisioned when the legislation was enacted.

The use of attributes will help insulate against changes in technology and allow the interception agency to focus on the aspects of the communication most likely to be of relevance to its investigation, saving time and resources and discarding product unconnected to the investigation, in effect leading to less intrusion into the privacy of other people.

Specific attributes can be used to identify and isolate particular communications or services which are more likely to be of security interest. This has the additional benefit of reducing the need to intrude into other communications which are unlikely to have relevance to security. In this way, attribute interception would be more privacy-neutral, and this addresses the concern some have expressed that technology-neutral legislation could have unintended detrimental effects on privacy.

Three case examples of the potential value of attribute interception are illustrative:

Case examples: the potential value of attribute interception

- Seeking telecommunications interception for a household of multiple people using a common internet service would intrude on each resident's privacy. An attribute-based approach would enable the communications of the single person of interest to be intercepted, based for example on a specific email address or known time of use.
- Cyber espionage actors have unique signatures associated with their activities: these are commonly known as intrusion sets. The ability to use attribute-based interception to intercept such content under warrant would significantly advance ASIO's ability to identify the scale and scope of activity by aggressive foreign intelligence actors, their targeting and priorities, and enable mitigation measures.
- When a new telecommunications service was introduced in the early 1990s it brought with it interception challenges. While a technical solution was developed within months of the technology being rolled out, use of that solution was not possible because the new technology did not fit the existing legislative definitions. The legislative change necessary to enable use of that technique took years. Attribute interception would have overcome such lags.

Data retention

Neither the TIA Act nor the Telecommunications Act define telecommunications data or require retention of it and so the accessibility of telecommunications data across service providers varies considerably. What the TIA Act does is require the information held to be provided to authorised agencies upon lawful request. ASIO is seeking amendments to the TIA Act to:

- ensure ASIO and law enforcement agencies can continue to access telecommunications data they need;
- describe clearly what telecommunications data should be retained for law enforcement or security purposes, without being exhaustively prescriptive (in accordance with the description of telecommunications data in Table 1); and
- require telecommunications providers to retain existing data for a specified period in a form readily accessible by agencies under appropriate authorisations.

This will address the key need for clarity and consistency across industry as to which telecommunications data will be retained and for how long.

In terms of data retention periods required for ASIO to effectively discharge its functions, at least two years is required in some cases, whether by carriers, carriage service providers, or ancillary service providers. Due to the nature of activity by clandestine foreign actors, retention for longer than two years would be ideal because of the following issues:

- While some security intelligence investigations are, like law enforcement investigations, a retrospective examination of a specific incident, the nature of clandestine or deceptive activity by foreign states against Australian interests, particularly by sophisticated adversaries, requires a different approach.
- Foreign states take a long-term, strategic approach to conducting espionage. The approach is slow and considered in order to hide activities. There is often no known or specific incident or starting point with espionage investigations. ASIO must baseline the activities and threat posed by adversaries over an extended period to identify indicators of activity and then review historical data to understand the extent and scope of the activity and harm. We note in the case of the European Union, their directive mandates data retention for up to two years.

Case studies can illustrate the need for such an approach, noting that ASIO could only achieve a security outcome in these cases because the telecommunications data happened to be held by the service providers, which is often not the case.

Case study: data retention identifies hostile cyber actors

- 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. Telecommunications 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 capabilities of the state-sponsored actor and the potential harm it was causing.

ASIO is cognisant of the security implications of the storage of personal data by telecommunications providers. The security of stored data would be a key priority. The Telecommunications Sector Security Reform initiatives proposed to the PJCIS in 2012 are intended to assist in mitigating risks around stored data. Those initiatives are aimed at not only addressing the national security risks to the sector but also providing a framework for better protecting the privacy of individual users. No decision has been made by the Government in relation to this initiative.

ASIO notes that the issue of telecommunications data access is not unique to Australia and has been the subject of review in a number of overseas jurisdictions (see Box 2 below, 'Overseas approaches to telecommunications data retention).

Box 2: Overseas approaches to telecommunications data retention

In the wake of the Snowden leaks, United States President Obama established a review group to look at intelligence access to and the collection of bulk telecommunications data. As a consequence of the review, President Obama has issued a Presidential Policy Directive which is intended to change the manner in which data is collected, stored and accessed by intelligence agencies. While the mechanics of the directive have yet to be worked out, there appear to be similarities to the current system in Australia. Bulk data would not be stored by the intercepting agency but rather by a third party (possibly the carriers) and accessed pending development of guidelines.

The European Union (EU) Data Retention Directive (2006/24/EC of 15 March 2006) provides one international model for mandatory data retention. The EU directive imposes an obligation for providers of publicly available electronic communications services and public communication networks to retain communications data for the purpose of the investigation, detection and prosecution of serious crime, as defined by each EU member state in national law. The EU directive requires the retention of subscriber and traffic data. There is no obligation on retention of the content of the communication. The directive was developed after the London and Madrid terrorist bombings and as a response to law enforcement and national security investigative needs. The EU Data Retention Directive has been implemented differently across the EU member states, with the most notable difference being who pays for the storage and access of the data. For example, the British Government pays all costs associated with data retention, whilst in Ireland the industry bears all the costs. Member states also differ in the retention periods they have agreed to, which can range from months to two years.

Obligations and standards for interception cooperation

Revised legislation also requires clarity, being legislation drafted in an accessible, unambiguous way to allow clear understanding of the obligations, responsibilities and requirement for access to data and interception.

ASIO remains cognisant of the need to provide clear and unambiguous advice to the telecommunications industry as to its obligations, how it can best contribute to protecting Australians from national security threats and serious criminal harm, and the consequences of noncompliance if some members of the industry are unwilling to assist. Judging from ASIO's

discussions with a number of carriers, they are willing to assist provided the obligations are applied to all members of the industry and are effectively enforced. This is often referred to as the desire for a 'level playing field'.

Frequently asked questions

Why does ASIO want to store all of Australia's telecommunications data?

There are many misconceptions in the public sphere around data retention, fuelled by speculation and inaccurate reporting. This includes the idea that data retention would result in the Australian Government, through agencies like ASIO, storing all telecommunications data to access at will. This is simply not true. Retained telecommunications data would continue to be held by the telecommunications carriers and accessed only when needed and when appropriate authorisations have been obtained.

Will data retention enable ASIO to monitor all Australians?

The public suggestion that the data retention proposal would allow ASIO and law enforcement agencies to monitor the communications of all Australians, such as web browsing, is incorrect. Such indiscriminate mass monitoring would not be possible under the proposal and ASIO does not seek it, nor would it be feasible. Nor would it (or should it) pass the scrutiny of the oversight and accountability mechanisms that apply to ASIO and law enforcement agencies.

Part 9—Discussion of the PJCIS and ALRC recommendations

The terms of reference for this inquiry refer to the recommendations made in two reports by the PJCIS and the ALRC:

- The PJCIS May 2013 *Report of the inquiry into potential reforms of Australia's national security legislation*, considered telecommunications interception (Chapter 2) and data retention (Chapter 5) and contains a number of recommendations relating to the TIA Act.
- The ALRC May 2008 report *For your information: Australian privacy law and practice*, considered telecommunications and privacy (Part J) and contains a number of recommendations relating to Part 13 of the Telecommunications Act and related provisions in the TIA Act.

The discussion in this part reflects the views of ASIO only for the purpose of responding to the inquiry's terms of reference. At the time of writing, the Government has made no decisions in relation to the comprehensive revision of the TIA Act, nor in relation to the recommendations contained in the Parliamentary Joint Committee of Intelligence and Security (PJCIS) report or Part J of the ALRC report.

ASIO's views in relation to each of the relevant PJCIS and ALRC recommendations follow in detail below. Comprehensive lists of the PJCIS and ALRC recommendations can be found at Annexures A and B respectively. There are a few recommendations in the PJCIS and ALRC reports on which ASIO has reservations. These relate to proposed changes to existing oversight and accountability mechanisms where ASIO believes existing arrangements and measures already cover the issues raised or where national security matters may be revealed. To emphasise

the distinction between telecommunications interception and data, ASIO's submissions in relation to the relevant recommendations have been presented under two headings: 'Telecommunications interception' and 'Telecommunications data'.

Part 9A - Telecommunications interception

ASIO largely supports the recommendations of the PJCIS and ALRC reports relating to telecommunications interception.

ASIO sees the value in the PJCIS recommendation to develop a single interception warrant regime to remove current unnecessary and unintended complexity. Importantly, the inclusion of proportionality considerations and accountability requirements in a single TI warrant regime would continue to deliver public confidence and assurance regarding the use of these powers.

ASIO is also seeking the ability to undertake 'attribute' interception. Rather than relying solely on a specific email address or telephone number, such attributes could include the location of the person making or receiving the call, or a specific communication signature. Attribute interception would allow for current interception capabilities to be applied to any new services which may emerge in the fast-paced telecommunications industry. Importantly, attribute interception could also be privacy-neutral by focusing interception on communications more likely to be of security interest and limiting incidental intrusion. This would be one approach to dealing with the concern some have expressed that technology-neutral legislation could have an unintended impact on privacy.

In summary, ASIO notes the following:

- In relation to proportionality, ASIO is already bound by the Attorney-General's Guidelines to consider proportionality and level of intrusion in its investigations and would not support a raising of the threshold (PJCIS Recommendations 2 and 10).
- ASIO would not support its activities falling within any public reporting requirements in the TIA Act and notes that the PJCIS did not explore the issue of extending these obligations to ASIO (PJCIS Recommendation 3).
- The ALRC report raised a proposal to establish a 'public interest' monitor. ASIO has reservations about this, if the effect would be simply to insert yet another approval step into the authorisation of a TI warrant. In ASIO's view, this function is already catered for in existing guidelines and oversight mechanisms (ALRC Recommendation 71-2).
- ASIO does not support the recommendations relating to additional legislative requirements regarding the destruction of intercepted content and additional reporting requirements (ALRC Recommendations 73-1, 73-2 and 73-4).

ASIO's reasons for reservations or not agreeing to a few of the recommendations are:

- they will not substantially add to or improve existing oversight and accountability mechanisms (ALRC Recommendations 71-2, 73-1 and 73-2); or
- ASIO's intelligence activities and capabilities need to be carried out with a degree of secrecy (ALRC Recommendation 73-4, PJCIS Recommendation 3).

PJCIS Recommendation 1: *The inclusion of an objectives clause within the TIA Act*

ASIO agrees that the inclusion of a clear objectives clause recognising investigative need as well as the protection of privacy is important in the TIA Act. It will be important in the drafting of the legislation to ensure clarity and a lack of ambiguity to avoid uncertainty in interpretation.

PJCIS Recommendation 2: *The Attorney-General's Department undertake an examination of the proportionality tests within the TIA Act*

ASIO is required by the Attorney-General's Guidelines to factor proportionality into investigative decision-making. This consideration is an important and integral part of ASIO investigative activity. In this way, proportionality is already a fundamental consideration of ASIO's access to telecommunications data and the content of communications.

We note the importance of ensuring that a proportionality test is appropriate to the relative privacy intrusion of the activity—seeking telecommunications data is not as intrusive as seeking the content of communications. ASIO submits any test or threshold for access to telecommunications data must ensure it meets privacy needs but allows law enforcement and security agencies to access data that in many cases resolves an investigation without requiring more intrusive investigative methods.

ASIO is concerned to ensure its ability to access telecommunications data continues with the appropriate internal authorisations and oversight, which includes consideration of the proportionality of the request, and subject to the independent oversight of the IGIS. Limiting or administratively burdening ASIO's ability to access this data represents a direct risk to our ability to effectively identify and investigate threats to Australia's security.

PJCIS Recommendation 3: *Revised TIA Act reporting requirements to ensure the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought*

The reporting requirements under the TIA Act do not relate to ASIO and the PJCIS did not explore the issue of extending these obligations to ASIO.

We emphasise the point made in paragraph 2.34 of the Committee's report which states: 'The Committee received assurance from the Commonwealth Ombudsman's office and the Inspector-General of Intelligence and Security of the high level of accountability discharged by the interception agencies'. Given this ongoing assurance provided by the Office of the IGIS in relation to the accountability of ASIO's activities, ASIO believes it important that our exclusion from those public reporting requirements remain. Publicly reporting on the nature and extent of ASIO's use of the TIA Act represents a threat to our ability to effectively operate. The nature of ASIO's security intelligence activities requires careful protection of our methods and the scope of our activity.

ASIO reports to the Attorney-General within three months of the expiry or revocation of a warrant issued under the TIA Act on the effectiveness of the warranted operation. ASIO notes the intrusive activity that indicates a negative risk to security is just as valuable as that which

indicates an immediate and real risk to security. Also, interception warrants are time specific and if a warrant is judged unlikely to produce further results it is formally revoked and not renewed.

The inspection and inquiry regime undertaken by the IGIS will continue to provide assurance to the Government and public that ASIO uses this, and other, investigative methods in a lawful and appropriate manner. Requirements such as these provide an important mechanism in demonstrating the appropriate and effective use of warranted powers.

PJCIS Recommendation 4: *Review of the oversight arrangements to ensure effective accountability under the TIA Act*

ASIO notes that this recommendation relates to law enforcement agencies and the consideration of state/territory and Commonwealth Ombudsman roles. ASIO's activities under the TIA Act remain monitored by the IGIS, who continues to report publicly to the Parliament on ASIO's use of the TIA Act powers. The PJCIS did not propose any reconsideration of the longstanding accountability and oversight arrangements for ASIO.

PJCIS Recommendation 6: *Examine the standardisation of thresholds for accessing the content of communications*

This recommendation relates to the different thresholds for law enforcement agencies to seek warrants enabling TI or to access stored communications. In relation to ASIO's use of these powers, the warrant thresholds in the TIA Act for seeking TI or access to stored communications are the same:

> **9 Issue of telecommunications service warrants by Attorney-General**
>
> (1) Where, upon receipt by the Attorney-General of a request by the Director-General of Security for the issue of a warrant under this section in respect of a telecommunications service, the Attorney-General is satisfied that:
>
> (a) the telecommunications service is being or is likely to be:
>
> (i) used by a person engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, activities prejudicial to security; or
>
> (ia) the means by which a person receives or sends a communication from or to another person who is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, such activities; or
>
> (ii) used for purposes prejudicial to security; and
>
> (b) the interception by the Organisation of communications made to or from the telecommunications service will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relating to security;
>
> (1A) The reference in paragraph (1)(b) to the interception of communications made to or from a telecommunications service includes a reference to the accessing of the communications as stored communications after they have ceased to pass over a telecommunications system.

ASIO maintains the references to 'prejudicial to security' in the thresholds reflects the privacy considerations of intercepting telecommunications content and the realistic need for ASIO to utilise this capability to investigate serious national security matters. It is a significantly higher threshold than 'relevant to security'.

PJCIS Recommendation 7: *Interception be conducted on the basis of specific attributes of communications*

A modernised telecommunications interception regime should allow agencies to 'intercept' but not dictate 'how' to intercept.

The TIA Act as currently written limits the technical means by which agencies can conduct interception by requiring interception be based on either a 'service' identifier (for example, a telephone number or email address) or a piece of 'equipment' (for example, a mobile telephone handset). This limits the method of interception. ASIO advocates the decoupling of the techniques for interception from the authorisation to intercept.

An alternative approach is attribute-based interception. 'Attributes' are specific identifying characteristics that can be used in combination to identify unique communications of interest to ASIO. Attribute-based interception encompasses service-based or equipment-based interception. It also allows ASIO to target specific attributes to collect communications of interest more effectively and less intrusively.

For example, some individual attributes that could be combined to enable better interception targeting could include:

- the source and/or destination of the communication;
- the type of communication (for example, a video call, email, SMS);
- the equipment being used to convey the communication (for example mobile telephone handset, cell tower);
- any identifier being used in connection with the communication (such as a number or username);
- a time period in which a communication is made or received; or
- the location of the person making or receiving the communication.

The selection of a combination of attributes in each particular case would involve a number of considerations, including the extent to which:

- the telecommunications provider had the ability to intercept the chosen attributes;
- attributes (singly or in combination) were sufficiently precise to give a high degree of certainty communications of interest are accessed; and
- certain components of a communication could be excluded on the basis they were likely to be irrelevant.

Attribute-based interception would allow agencies to filter and limit the communications they intercept more efficiently, helping to minimise the collection of extraneous information. With this more specific method of targeting the telecommunications of interest, the more certain we can be that we are excluding from incidental interception the communications of persons who are not of interest and whose privacy should be protected.

As noted in the PJCIS report, ASIO views attribute-based interception as one of many elements required in order to address the decline in telecommunications interception capability. ASIO agrees with the PJCIS findings that the accountability and oversight of this method will be important, but should be covered by existing accountability and oversight mechanisms.

PJCIS Recommendation 8: *Review the information sharing provisions of the TIA Act*

ASIO supports the recommendation and believes this is particularly important in the modern communications environment, given the national and transnational nature of law enforcement and security investigations where effective cooperation within and between agencies is essential.

In relation to ASIO, the TIA Act in combination with the ASIO Act currently provides appropriate restrictions: ASIO may communicate intercepted information in connection with the performance of its functions or otherwise for purposes of security. ASIO may also communicate intercepted information:

- to a minister, authority of the Commonwealth, or authority of the state, where the information appears to relate to their functions and a serious crime or the national interest requires the communication;
- to ASIS, ASD or AGO where the information relates or appears to relate to the performance of their functions; and
- pursuant to a cooperation arrangement entered into under section 19A of the ASIO Act.

PJCIS Recommendation 9: *Remove legislative duplication from the TIA Act*

Over time, the many amendments to the TIA Act have resulted in duplication and complexity making the Act difficult to understand and apply. Conversely, there is intentional duplication for provisions that apply specifically to ASIO with separate provisions for enforcement agencies. For example, voluntary disclosure provisions for ASIO are covered under section 174 whereas section 177 relate to enforcement agencies.

ASIO supports the recommendation to remove legislative duplication but notes it should not be applied in instances where there is a necessary distinction between ASIO's security intelligence role and law enforcement agencies.

PJCIS Recommendation 10: *The telecommunications interception warrant provisions in the TIA Act be revised to develop a single interception warrant regime*

ASIO's use of TI and access to communications is subject to a strict legislative and policy oversight and accountability regime. Existing accountability mechanisms have proved to be effective in ensuring ASIO acts with legality and propriety in executing telecommunications interception powers.

For ASIO, the TIA Act currently differentiates between four warrant categories with discrete legislative tests to be satisfied before an interception capability can be used to obtain intelligence relevant to security. This complexity is a direct result from changes in technology and the

telecommunications environment and has resulted is an inefficient and costly process for agencies, issuing authorities, and industry.

Overall, ASIO supports the recommendation to develop a single interception warrant regime to remove current unnecessary and unintended complexity. Importantly, the maintenance of the proportionality thresholds and accountability requirements in a single TI warrant regime would continue to deliver public confidence and assurance regarding the use of these powers.

The PJCIS noted (2.111) the necessary balance between appropriate checks and balances and the operational flexibility required to deliver effective law enforcement and protection against national security threats. The reduction in complexity delivered through a single interception warrant regime would provide ASIO with a more agile operational capability, within an appropriate accountability framework.

In relation to the recommendation that interception be authorised only when the Attorney-General is satisfied it would be proportionate to the national security threat being investigated, it depends on what would be proposed but ASIO notes it is already bound by the Attorney-General's Guidelines to consider proportionality in its investigations and sees no need to raise an already appropriate threshold.

PJCIS Recommendation 11: *Review the application of the interception-related industry assistance obligations in the TIA Act and the Telecommunications Act*

ASIO supports the recommendation to provide certainty and clarity as well as provide a more flexible approach.

ASIO notes interception agencies have experienced considerable difficulty with the existing TIA Act interception capability/delivery capability cost-sharing model. This has been due to a combination of:

- existing definitions of interception capability, delivery capability and delivery point(s) which are not a good fit with contemporary Internet Protocol-based technology, and do not embrace important international lawful interception concepts;
- compliance with TIA Act obligations and the ability to enforce them;
- inefficient administrative mechanisms for refunding costs for the development, installation and maintenance of delivery capabilities;
- the artificial split between interception capability and delivery capability to enable cost allocation when in fact they are a complete end-to-end system; and
- lack of certainty that carriers may not profit from the provision of delivery capabilities. This is particularly acute in cases where private vendors are being used for the purposes of developing delivery capabilities which they do at profit.

ASIO's view is that clarity around obligations will facilitate enhanced understanding, and enable appropriate enforcement action in the event of non-compliance. In order to address the dynamic nature of communications technology, there also must be flexibility to allow industry and agencies to work together in ways that cannot be anticipated now. Additionally, ASIO believes a

successful regime must include a mechanism to share reasonable costs between Government and telecommunication companies. This is necessary to reflect the cooperative partnership that must exist to ensure effective operational outcomes.

PJCIS Recommendation 12: *Consider expanding the regulatory enforcement options available to ACMA to include a range of enforcement mechanisms in order to provide tools proportionate to the conduct being regulated*

ASIO supports the recommendation noting it should avoid unnecessarily exposing sensitive methodology or lack of interception capability.

The current regulatory and enforcement framework has impeded the ability to undertake necessary and appropriate enforcement action. This stems in part from the absence of clarity around industry obligations but also relates to the absence of targeted sanctions for noncompliance.

A greater range of proportionate enforcement options would appear to be more effective than the current regime, which lacks 'middle-order' options to address cases of serious noncompliance in cases where court action would be inappropriate. Such action has the operational consequence of unduly publicising the lack of an effective interception capability and is not conducive to short-term resolution required by agencies. The consequences of public disclosure of potential gaps in ASIO's interception capabilities would be significant, and would undermine its ability to effectively identify and investigate threats to security.

PJCIS Recommendation 13: *Amend the TIA Act to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies*

ASIO supports the recommendation and agrees such amendments would provide greater certainty and clarity for the telecommunications industry and interception agencies. Any revision must provide flexibility to address the impact of technology and business change that cannot be anticipated now.

Industry, together with intercepting agencies, spends significant resources to develop and maintain effective interception capabilities. Implementations vary between networks and require updating as technology, the environment and requirements change. Importantly, the complexities associated with modern communication networks and services mean general obligations are, on their own, no longer effective and create an environment of ambiguity and ineffectiveness.

Implementation of detailed interception and delivery capability requirements for industry interception obligations should assist in addressing issues including delivery of information in a useable form, within specified timeframes and subject to specified security standards. Additionally, provision should be made to respond appropriately to a constant and rapidly changing environment.

PJCIS Recommendation 14: *Amend the TIA Act and the Telecommunications Act to make it clear that existing obligations apply to all providers (including ancillary service providers) of services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers*

ASIO supports the recommendation—it will provide much needed clarity.

It is important Australia does not provide potential safe havens, or methods of communication which are not subject to clear obligations to assist ASIO. Otherwise, the consequence would be for individuals of security interest to hide their activities from security intelligence view due to inadvertent legislative ambiguity.

ASIO believes ancillary providers should also be subject to the same cost-sharing arrangements as other telecommunications providers.

PJCIS Recommendation 15: *The Government should develop the implementation model on the basis of a uniformity of obligations while acknowledging that the creation of exemptions on the basis of practicability and affordability may be justifiable in particular cases. However, in all such cases the burden should lie on the industry participants to demonstrate why they should receive these exemptions*

ASIO supports this recommendation.

ASIO supports a regime where obligations are made clear to telecommunications providers on the level of support and interception capability they are required to develop and maintain. ASIO is seeking a regime enabling it to provide clarity for industry on the nature and extent of interception capability required.

ASIO notes this provision must come with an effective regulatory regime to provide enforcement of interception and assistance obligations, which are significant issues in the current framework.

PJCIS Recommendation 16: *Should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations*

ASIO supports the need to clarify with telecommunications providers their obligations to assist in decrypting communications. This is a longstanding requirement that has become more important as the prevalence of encryption has increased. The 2005 *Report of the review of the regulation of access to communications* by Mr Anthony Blunn noted (at para 4.6) that to remain effective, interception requires that the agency be provided with the content of communications

in useable form—in a form that can be read, listened to, or used in evidence. Such a provision will be important in allowing agencies access to information in a form that is accessible and appropriate to support investigations.[17] ASIO continues to support this finding from the report.

PJCIS Recommendation 17: *If the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. The cost to the telecommunications industry must be considered.*

ASIO supports the recommendation and welcomes the opportunity for wider consultation.

ASIO's work includes emergency response to provide advice and prevent security incidents. It is essential telecommunications providers deal with assistance requests from ASIO and law enforcement agencies in a timely manner, particularly urgent requests.

This is particularly important given the lack of uniform retention periods for telecommunications data where delays in actioning requests could result in loss of critical intelligence or lead information. Similarly, any delays to executing ASIO's telecommunications interception warrants undermines our ability to effectively counter threats to security and protect the community.

ASIO understands there may be technical and procedural factors affecting timeliness and is not seeking to implement unreasonable or disproportionate timeframes.

PJCIS Recommendation 18: *The TIA Act be comprehensively revised*

ASIO supports this recommendation. Our views on the need for modernisation are detailed in Parts 7 and 8 of this submission.

ALRC Recommendation 71-2: *Review of the effectiveness of the Telecommunications Act and the TIA Act*

ASIO supports an holistic review of the TIA Act and relevant parts of the Telecommunications Act to ensure they continue to be effective in light of technological developments, changes in the structure of communication industries and changing community perceptions and expectations about communication technologies.

In the absence of significant and timely modernisation, law enforcement and national security agencies face the prospect of continuing progressively to lose integral intelligence and evidentiary collection capabilities—commonly referred to as 'going dark'.

Any revision of the regulatory regime should provide for the following:

[17] The report is available online from the Attorney-Generals' website, www.ag.gov.au

- capability to identify and collect communications of security relevance;
- clarified obligations to provide certainty to the telecommunications industry and Government about the nature and scope of the assistance to be provided when investigating threats to national security and serious criminal offences;
- principles-based, technology-neutral provisions to decouple interception and access capability from current day technologies to ensure the regime (and therefore agencies) can respond with agility and flexibility to future technical developments;
- administrative efficiency to reduce the operational opportunity cost associated with the administration of the telecommunications interception and access regime while maintaining public confidence in the application of the interception and access regime; and
- appropriate use for lawful purposes of telecommunications interception and access to telecommunications data within an efficient and effective accountability framework that does not impede agile operational decision-making.

Public interest monitor

In light of current accountability, oversight and proportionality mechanisms already in place, ASIO has reservations about the potential value of an amendment of the TIA Act to provide for a new role of a public interest monitor in respect of the security intelligence function. The ALRC asked whether the role of a monitor should include:

- appearing at any application made by an agency for interception and access warrants under the Act;
- testing the validity of warrant applications;
- gathering statistical information about the use and effectiveness of warrants;
- monitoring the retention or destruction of information obtained under a warrant;
- providing to the IGIS, or other authority as appropriate, a report on noncompliance with the Act; or
- reporting to the Australian Parliament on the use of interception and access warrants (p.2509).

As recognised by the ALRC in its report, many of the functions of a public interest monitor are adequately provided by other bodies (p. 2,394 and 2,510). ASIO supports this view and notes a combination of existing accountability mechanisms already address (see page 18) the potential roles the ALRC considered for a monitor. ASIO notes the concerns expressed by the Attorney-General's Department to the ALRC at the time that the introduction of a monitor to a request for activity could raise questions about the integrity and independence of the issuing authority (p.2510).

ASIO acknowledges and supports the need for appropriate and thorough consideration of the privacy implications of proposals to use intrusive telecommunications interception techniques against persons of interest. Privacy considerations already inform ASIO's security intelligence investigations, through application of the Attorney-General's Guidelines as described earlier in this submission.

In ASIO's view, the existing accountability mechanism are sufficient and a monitor would be an additional layer of bureaucracy without providing a unique public value above what presently exists, including the role of the Inspector-General of Intelligence and Security. If the TIA Act were to provide for a public interest monitor for all interception agencies, the role and functions of the monitor in relation to ASIO would need to be carefully considered in light of the provisions of the IGIS Act and ASIO Act.

ALRC Recommendation 71-4: *Development of guidance that addresses privacy issues raised by new technologies*

ASIO supports the development of guidance to address privacy issues raised by new technologies, provided this is undertaken in consultation with law enforcement and national security agencies, as well of those agencies representing privacy interests.

The development of such guidance needs to be undertaken in parallel with the review of the legislative framework to ensure it is as technologically neutral as possible.

ASIO notes the suggestion of the ALRC in Chapter 10 of its report that the most effective way to ensure privacy protection in light of developing technology is to ensure the Privacy Act is technology-neutral. The same argument applies in respect of Part 13 of the Telecommunications Act and the TIA Act—that is, the TIA Act and Telecommunications Act will also only continue to remain effective in the future if they are technology-neutral.

ALRC Recommendations 71-5 and 71-6: *Requirement for ACMA to consult with Privacy Commissioner before registering codes and determining industry standards dealing directly or indirectly with a matter dealt with by the Privacy Act*

ASIO supports the need for the Australian Communications and Media Authority (ACMA) to consult with the Privacy Commissioner to ensure privacy concerns are appropriately considered before registering codes and making industry standards. ASIO believes it is also important for consultation to be undertaken with other relevant stakeholders to ensure interests in addition to privacy are also appropriately canvassed.

ALRC Recommendation 73-1, 73-2: *Destruction of records – intercepted material, destruction of non-material content intercepted under a B-Party warrant*

ASIO has responsibilities to retain records under the *Archives Act 1983*. At the same time, ASIO has an overriding obligation to destroy records and copies of communications intercepted under a telecommunications interception warrant where:

- the record or copy is in the possession or custody, or under the control of ASIO; and
- the Director-General of Security is satisfied that the record or copy is not required, and is not likely to be required, in or in connection with the performance of ASIO's functions or the exercise of its powers.

ASIO has additional relevant requirements under the Attorney-General's Guidelines to:

- destroy records of an inquiry or investigation where the subject's activities are not, or are no longer, relevant to security, under disposal schedules agreed to between ASIO and the National Archives of Australia; and
- only use, handle or disclose personal information where reasonably necessary for the performance of its statutory functions or as otherwise authorised, or required by law.

ASIO's compliance with these requirements is subject to oversight by the IGIS.

ASIO submits that amendment of the TIA Act to include additional legislative requirements regarding the destruction of intercepted content is unnecessary.

ALRC Recommendation 73-4: *Reporting requirements regarding stored communications warrants*

ASIO reports to the Attorney-General within three months of the expiry or revocation of a warrant issued under the TIA Act on the effectiveness of the warranted operation. Requirements such as these provide an important mechanism in demonstrating the appropriate and effective use of warranted powers.

Adding to existing reporting requirements would not necessarily result in more meaningful oversight and accountability of the use of warranted powers.

ASIO notes the proposed reduction in reporting requirements as part of the reforms to the TIA Act considered by the PJCIS, as well as the PJCIS recommendation for examination of the reporting requirements in the TIA Act to ensure the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.

ALRC Recommendation 73-7: *Addition of Office of Privacy Commissioner as member of Law Enforcement Advisory Committee*

ASIO supports and acknowledges the importance of ensuring that the privacy impact of policy proposals of law enforcement and national security issues relating to telecommunications are given appropriate weight.

ALRC Recommendation 73-8 and 73-9: *Development of memorandums of understanding between ACMA, TIO and Office of the Privacy Commissioner, and Office of the Privacy Commissioner—complaint-handling policies and procedures and enforcement guidelines*

ASIO supports measures aimed at clarifying and strengthening the relationships between the various bodies with responsibility for telecommunications regulation. Such measures are also likely to result in a reduction in unnecessary duplication in this area and provide greater certainty for industry and consumers regarding the role and functions of each of these bodies.

ALRC Recommendation 73-10 and 73-11: *Development of guidance by ACMA relating to privacy in the telecommunications industry, and development of public educational material by ACMA*

ASIO supports the development of guidance and public education material by ACMA, provided this is undertaken in consultation with all relevant stakeholders, including law enforcement and national security agencies.

Part 9B—Telecommunications data

In addition to considering telecommunications interception, the PJCIS made two recommendations specifically relating to telecommunications data and the ALRC report made recommendations relating to:

- Part 13 of the *Telecommunications Act 1997*, which restricts the ability of telecommunications service providers to use and disclose certain types of information, including telecommunications data; and
- access to and use of such information by ASIO and law enforcement agencies under the TIA Act.

There would be potential impost on carriers, carriage service providers and internet service providers from a requirement to hold essential telecommunications data for a specified time. Network data to ensure a communication is sent to the right party will always be required by the provider. We do not ask that they create new data; rather we ask that they retain existing data for a reasonable time in the event it assists future investigations. ASIO supports the PJCIS recommendation that the current cost-sharing arrangements be maintained and extended to ancillary service providers.

The main area of contention appears to rest in the area of access to, use of and retention of telecommunications data. There is a significant public misconception regarding data retention, fuelled by media reporting of how the US intelligence system operates, that ASIO is seeking direct access to the telecommunications data of all Australians. This is not the case. ASIO remains of the view the data retention scheme should operate by telecommunications data continuing to be stored by the provider or ancillary service provider and being accessed only when required based on a formal request to a provider. This request itself should be based on duly documented and authorised processes by the requesting agency. The whole process should be subject to formal oversight by an external entity—in ASIO's case, this is the IGIS.

This submission explains how and why the collection and analysis of specific telecommunications 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. This issue has been the subject of recent public debate stemming from leaks by former US National Security Agency (NSA) contractor, Edward Snowden. To this end, the submission has endeavoured to make ASIO's activities clear in the context of this debate. In short, ASIO seeks no change to the rules for access to and use of telecommunications data for national security purposes, but would like to see the obligations for retention of that data for a specified period prescribed in law.

In summary, ASIO largely supports the recommendations of the PJCIS and ALRC reports relating to telecommunications data but notes the following:

- ASIO supports a technology-neutral definition of telecommunications data and would not support an exhaustive definition with the potential for unintended consequences in limiting access to telecommunications data (ALRC Recommendation 73-5).
- ASIO partly supports the recommendation relating to guidance on interception and access to information under the TIA Act (ALRC Recommendation 73-5). ASIO would welcome such guidance but it should not be publicly available.
- ASIO does not support the recommendations relating to additional legislative requirements regarding the destruction of telecommunications data and additional reporting requirements as it will not substantially add to or improve existing oversight and accountability mechanisms (ALRC Recommendation 73-3).

PJCIS Recommendation 5: *Review the threshold for access to telecommunications data*

The PJCIS was satisfied access by law enforcement agencies and ASIO to telecommunications data for serious crime and threats to security is justified. This recommendation does not propose to alter ASIO's ability or threshold to access to telecommunications data.

ASIO notes the Committee expressed concerns regarding the present definition of enforcement agency, leaving the potential for many agencies to request access to telecommunications data without independent scrutiny other than from the telecommunications providers who receive those requests. ASIO does not fall into the category of agencies recommended for further review by the Committee, which noted '*access for agencies not enforcing the criminal law or investigating security threats should be subject to further review'*.

PJCIS Recommendation 42: *Mandatory data retention regime*

As previously outlined in the joint supplementary submission to the PJCIS *Inquiry into Potential Reforms of Australia's National Security Legislation* by ASIO, AFP and ACC, Part 5 of this submission defines our understanding of the scope of telecommunications data for which ASIO is seeking mandatory retention and Part 8 puts our views on the need for a mandatory data retention regime.

ALRC Recommendation 71-1: *Redrafting of Part 13 of the Telecommunications Act 1997*

ASIO supports the redrafting of Part 13 of the Telecommunications Act to achieve greater logical consistency, simplicity and clarity as part of an overall review of the effectiveness of the TIA Act and related parts of the Telecommunications Act.

ALRC Recommendation 71-3: *Amendment of Telecommunications Act 1997 to include civil penalties*

ASIO acknowledges and supports the need for strong and effective protection of information held by the telecommunications industry. Amendments to provide for civil as well as criminal penalties for the unauthorised use or disclosure of this information may assist in ensuring compliance with legislative requirements.

ASIO supports a greater range of proportionate enforcement mechanisms being available to ACMA, which together with clearly defined industry obligations (including in relation to the security of telecommunications interception product and timeliness of assistance) will enable more targeted sanctions for noncompliance.

Exceptions to the use and disclosure offences

ALRC Recommendations 72-1 to 72-9: *Exceptions to the use and disclosure offences*

ASIO supports amendment of Part 13 of the Telecommunications Act to ensure access to and use of information held by the telecommunications industry is only authorised for limited legitimate purposes, including the enforcement of the criminal law and safeguarding of Australia's national security. The lack of clarity regarding the scope of the current exceptions to the use and disclosure offences significantly impacts on the effectiveness of Part 13 in ensuring the appropriate protection of this information.

ASIO obtains access to information protected under Part 13 of the Telecommunications Act through authorisations issued under sections 175 and 176 of the TIA Act. Such authorisations can only be made where the authorised officer is satisfied, on a case-by-case basis that the disclosure of the particular information would be in connection with the performance by ASIO of its functions. In the case of access to prospective information or documents, authorisation is required from an officer at the SES Band 2 level or above.

ASIO's access to information under data authorisations is subject to stringent oversight by the IGIS who undertakes regular inspections of a significant number of ASIO investigations and operational activities.

ALRC Recommendation 72-6: *Cross-reference to the TIA Act*

ASIO supports amendments to clarify the relationship between the TIA Act and Part 13 of the Telecommunications Act to provide further certainty regarding ASIO's access to information protected under Part 13.

ALRC Recommendation 72-10: *Credit reporting information*

ASIO acknowledges and supports the need to ensure the use and disclosure of information relating to an individual's credit worthiness is appropriately protected.

ASIO relies upon a wide range of information held by carriers and carriage service providers in undertaking security investigations, including information relating to the billing or payment information of their customers. ASIO's access to such information is limited to those circumstances where a clearly defined need and justification exists for accessing such information, and authorisation has been given in accordance with Chapter 4 of the TIA Act.

It is important any legislative changes in this area do not adversely impact the ability of ASIO and law enforcement agencies to continue to access critical information from carriers and carriage service providers.

ALRC Recommendation 72-11 to 72-16: *Integrated Public Number Database related recommendations*

Telstra maintains and manages the Integrated Public Number Database (IPND) as part of its carrier licence conditions. It lists every telephone number, the name and address of the person who uses it, and the telephone company who provided it to them. One of the primary reasons for the establishment and maintenance of the IPND (as set out in the *Carrier Licence Condition (Telstra Corporation Limited) Declaration 1997 (Cth)*) is to assist enforcement agencies and safeguard national security.

It is critical ASIO continues to be able to access IPND data under mechanisms similar to those currently available. ASIO acknowledges and supports the need for certainty about when use or disclosure of information or a document held on the IPND is permitted. Access to information contained in the IPND and other similar directory products is, and should be, limited to those circumstances where a clearly defined need and justification exists for accessing such information, including the enforcement of the criminal law and safeguarding national security.

In the same way, the ALRC recommended reviewing the continued effectiveness of the Telecommunications Act and TIA Act in light of technological developments and changes to industry structure, ASIO supports updating the IPND and associated industry regulations to include information on IP access services and associated customer and technical details. The IPND remains a critical tool for law enforcement, national security and emergency services agencies: however, it does not reflect changing technology and ubiquitous use of the internet. ASIO believes an internet equivalent to the IPND is critical to enabling effective, secure internet investigations into the future. The establishment of this reference index, with appropriate privacy and access protections as currently in place with the IPND, would enable ASIO and law enforcement agencies to identify which internet service provider is providing internet services to an individual under investigation.

ALRC Recommendation 73-3: *Destruction of irrelevant material containing accessed telecommunications data by ASIO and law enforcement agencies*

As outlined in more detail above in relation to recommendations 73-1 and 73-2, amendment of the TIA Act to include additional legislative requirements regarding the destruction of telecommunications data is unnecessary due to the adequacy of existing requirements.

ALRC Recommendation 73-5: *Guidance on interception and access to information under the TIA Act to be developed by the Attorney-General's Department*

ASIO already works closely with the Attorney-General's Department and law enforcement agencies to ensure consistency in application of the TIA Act where appropriate. Although ASIO supports the development of guidance on interception and access of information under the TIA Act by the Attorney-General's Department, it does not support such guidance being publicly available. Guidance relating to the TIA Act will contain sensitive information relating to the capabilities of ASIO or law enforcement agencies and needs to be protected from public disclosure.

Definition of telecommunications data

ASIO would prefer that telecommunications data is defined in the TIA Act using broad categories, such as in Table 1 earlier in this submission, rather than in exhaustive detail. This would assist the legislation to keep pace with changes in technology. This was recognised by the ALRC who did not recommend amending the TIA Act to define telecommunications data on the basis that the exclusion of a definition enables the legislation to remain technology-neutral so it can be applied to new developments in technology without the need for amendment.

It is essential the introduction of a definition of telecommunications data into the TIA Act does not adversely impact ASIO's ability to access all information currently able to be accessed under authorisations issued under the TIA Act. Any proposal to limit (including through the inclusion of an exhaustive definition of telecommunications data) the type of information that can be accessed under a section 175 or section 176 authorisation needs to take into account the scope of the prohibition on disclosure in Part 13 of the Telecommunications Act.

Voluntary disclosure

Carriers and carriage service providers are currently authorised to disclose information or a document to ASIO if the disclosure is in connection with ASIO's functions. On the other hand, where carries are aware of a specific interest by ASIO in the form of a request for telecommunications data made by ASIO, carriers are not permitted voluntarily to disclose additional information beyond the terms of the request. In circumstances where carriers are aware there is other relevant information they are able to make ASIO aware of that fact to enable ASIO to make a further request.

The ability for carriers and carriage service providers voluntarily to disclose information would assist providers in complying with their obligations under Part 14 of the Telecommunications Act. Removing or limiting the ability of carriers and carriage service providers to voluntarily disclose information to ASIO and law enforcement agencies would undermine the ability of agencies to detect and investigate a range of crimes including cybercrimes and national security threats that come to the attention of carriers and carriage service providers.

Timeframes for destruction

Any guidance addressing the timeframes within which agencies should review holdings of information and destroy information must take into account the differences between the nature of law enforcement and ASIO investigations, and in particular, ASIO's intelligence collection role versus law enforcement's evidentiary collection role.

ALRC Recommendation 73-6: *Requirement to provide information to the Ombudsman*

As recognised by the ALRC, a legislative amendment to provide that the IGIS monitor the use of powers by ASIO is unnecessary. The IGIS reviews ASIO's access to information under data authorisations as part of regular inspections of ASIO investigations.

*
**

Annexure A—PJCIS recommendations verbatim

2 Telecommunications Interception	
1	The Committee recommends the inclusion of an objectives clause within the *Telecommunications (Interception and Access) Act 1979*, which: • expresses the dual objectives of the legislation – - to protect the privacy of communications; - to enable interception and access to communications in order to investigate serious crime and threats to national security; and • accords with the privacy principles contained in the *Privacy Act 1988*.
2	The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the *Telecommunications (Interception and Access) Act 1979* (TIA Act). Factors to be considered in the proportionality tests include the: • privacy impacts of proposed investigative activity; • public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and • availability and effectiveness of less privacy intrusive investigative techniques. The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.
3	The Committee recommends that the Attorney-General's Department examine the *Telecommunications (Interception and Access) Act 1979* with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.
4	The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the *Telecommunications (Interception and Access) Act 1979*. Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism. The Committee also recommends the Attorney-General's Department consult with State and Territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.
5	The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.

6	The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the: • privacy impact of the threshold; • proportionality of the investigative need and the privacy intrusion; • gravity of the conduct to be investigated by these investigative means; • scope of the offences included and excluded by a particular threshold; and • impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.
7	The Committee recommends that interception be conducted on the basis of specific attributes of communications. The Committee further recommends that the Government model 'attribute based interception' on the existing named person interception warrants, which includes: • the ability for the issuing authority to set parameters around the variation of attributes for interception; • the ability for interception agencies to vary the attributes for • interception; and • reporting on the attributes added for interception by an authorised officer within an interception agency. In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures: • attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated; • oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and • reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.
8	The Committee recommends that the Attorney-General's Department review the information sharing provisions of the *Telecommunications (Interception and Access) Act 1979* to ensure: • protection of the security and privacy of intercepted information; and • sharing of information where necessary to facilitate investigation of serious crime or threats to national security.
9	The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.

10	The Committee recommends that the telecommunications interception warrant provisions in the *Telecommunications (Interception and Access) Act 1979* be revised to develop a single interception warrant regime. The Committee recommends the single warrant regime include the following features: • a single threshold for law enforcement agencies to access communications based on serious criminal offences; • removal of the concept of stored communications to provide uniform protection to the content of communications; and • maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises. The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures: • interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated; • rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security; • reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and • Parliamentary oversight of the use of interception.
11	The Committee recommends that the Government review the application of the interception-related industry assistance obligations contained in the *Telecommunications (Interception and Access) Act 1979* and *Telecommunications Act 1997*.
12	The Committee recommends the Government consider expanding the regulatory enforcement options available to the Australian Communications and Media Authority to include a range of enforcement mechanisms in order to provide tools proportionate to the conduct being regulated.
13	The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.
14	The Committee recommends that the *Telecommunications (Interception and Access Act) 1979* and the *Telecommunications Act 1997* be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including ancillary service providers) of telecommunications services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers.
15	The Committee recommends that the Government should develop the implementation model on the basis of a uniformity of obligations while acknowledging that the creation of exemptions on the basis of practicability and affordability may be justifiable in particular cases. However, in all such cases the burden should lie on the industry participants to demonstrate why they should receive these

	exemptions.
16	The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations.
17	The Committee recommends that, if the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. The Committee further recommends that, if the Government decides to develop mandatory timelines, the cost to the telecommunications industry must be considered.
18	The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following: • clear protection for the privacy of communications; • provisions which are technology-neutral; • maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes; • clearly articulated and enforceable industry obligations; and • robust oversight and accountability which supports administrative efficiency. The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies. The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the: • Independent National Security Legislation Monitor; • Australian Information Commissioner; • ombudsmen and the Inspector-General of Intelligence and Security. • In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.
5 Data Retention	
42	There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a

	mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features: • any mandatory data retention regime should apply only to metadata and exclude content; • the controls on access to communications data remain the same as under the current regime; • internet browsing data should be explicitly excluded; • where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access; • the data should be stored securely by making encryption mandatory; • save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years; • the costs incurred by providers should be reimbursed by the Government; • a robust, mandatory data breach notification scheme; • an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and • oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.
43	The Committee recommends that, if the Government is persuaded that a mandatory data retention regime should proceed: • there should be a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security; • there should be an annual report on the operation of this scheme presented to Parliament; and • the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement.

Annexure B—ALRC recommendations verbatim

Extracts from the ALRC's report For Your Information: Australian Privacy Law and Practice.

71. Telecommunications Act	
71–1	Part 13 of the Telecommunications Act 1997 (Cth) should be redrafted to achieve greater logical consistency, simplicity and clarity.
71–2	The Australian Government should initiate a review to consider whether the Telecommunications Act 1997 (Cth) and the Telecommunications (Interception and Access) Act 1979 (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider: (a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services; (b) how these two Acts interact with each other and with other legislation; (c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation; (d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance; and (e) whether the Telecommunications (Interception and Access) Act should be amended to provide for the role of a public interest monitor.
71–3	The Telecommunications Act 1997 (Cth) should be amended to provide that a breach of Divisions 2, 4 and 5 of Part 13 of the Act may attract a civil penalty in addition to a criminal penalty. The Australian Communications and Media Authority should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil or a criminal penalty is made.
71–4	The Australian Communications and Media Authority, in consultation with the Office of the Privacy Commissioner, Communications Alliance, the Telecommunications Industry Ombudsman, and other relevant stakeholders, should develop and publish guidance that addresses privacy issues raised by new technologies such as location-based services, voice over internet protocol and electronic number mapping.
71–5	Section 117(1)(k) of the Telecommunications Act 1997 (Cth) should be amended to provide that the Australian Communications and Media Authority cannot register a code that deals directly or indirectly with a matter dealt with by the Privacy Act, or an approved privacy code under the Privacy Act, unless it has consulted with, and taken into consideration any comments or suggested amendments of, the Privacy Commissioner.

71–6	Section 134 of the Telecommunications Act 1997 (Cth) should be amended to provide that the Australian Communications and Media Authority cannot determine or vary an industry standard that deals directly or indirectly with a matter dealt with by the Privacy Act, or an approved privacy code under the Privacy Act, unless it has consulted with, and taken into consideration any comments or suggested amendments of, the Privacy Commissioner.
72. Exceptions to the Use and Disclosure Offences	
72–1	Sections 280(1)(b) and 297 of the Telecommunications Act 1997 (Cth) should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the Privacy Act if that use or disclosure would not be otherwise permitted under Part 13 of the Telecommunications Act.
72–2	The Telecommunications Act 1997 (Cth) should be amended to provide that a use or disclosure of information or a document is permitted if a person has reason to suspect that unlawful activity has been, is being, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.
72–3	The Telecommunications Act 1997 (Cth) should be amended to provide that a telecommunications service provider may use or disclose 'personal information' as defined in the Privacy Act about an individual who is an existing customer aged 15 or over for the purpose of direct marketing only where the: (a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; (b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and (c) the information does not relate to the contents of a communication carried, or being carried, by a telecommunications service provider; or carriage services supplied or intended to be supplied by a telecommunications service provider.
72–4	The Telecommunications Act 1997 (Cth) should be amended to provide that a telecommunications service provider may use or disclose 'personal information' as defined in the Privacy Act about an individual who is an existing customer and is under 15 years of age for the purpose of direct marketing only in the following circumstances: (a) either the: (i) individual has consented; or (ii) information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure; and (b) the information does not relate to the contents of a communication carried, or being carried, by a telecommunications service provider; or carriage services supplied or intended to be supplied by a telecommunications service provider;

	(c) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications; (d) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and (e) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.
72–5	The Telecommunications Act 1997 (Cth) should be amended to provide that in the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must: (a) comply with this requirement within a reasonable period of time; and (b) not charge the individual for giving effect to the request.
72–6	A note should be inserted after s 280 of the Telecommunications Act 1997 (Cth) cross-referencing to Chapter 4 (Access to telecommunications data) of the Telecommunications (Interception and Access) Act 1979 (Cth).
72–7	Sections 287 and 300 of the Telecommunications Act 1997 (Cth) should be amended to provide that a use or disclosure by a 'person', as defined under the Act, of information or a document is permitted if: (a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and (b) the person reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to a person's life, health or safety.
72–8	Section 289 of the Telecommunications Act 1997 (Cth) should be amended to provide that a use or disclosure by a 'person', as defined under the Act, of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and (a) the other person has consented to the use or disclosure; or (b) the use or disclosure is made for the purpose for which the information or document came to the person's knowledge or into the person's possession (the primary purpose); or (c) the use or disclosure is for a purpose other than the primary purpose (the secondary purpose); and (i) the secondary purpose is related to the primary purpose, and if the information or document is sensitive information (within the meaning of the Privacy Act), the secondary purpose is directly related to the primary purpose; and (ii) the other person would reasonably expect the person to use or disclose the

	information.
72–9	Part 13 of the Telecommunications Act 1997 (Cth) should be amended to provide that 'consent' means 'express or implied consent'.
72–10	Part 13 of the Telecommunications Act 1997 (Cth) should be amended to provide that use or disclosure by a person of credit reporting information is to be handled in accordance with the Privacy Act.
72–11	The Telecommunications Act 1997 (Cth) should be amended to clarify when a use or disclosure of information or a document held on the integrated public number database is permitted.
72–12	Clause 3 of the Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997 (Cth) should be amended to provide that 'enforcement agency' has the same meaning as that provided for in the Telecommunications (Interception and Access) Act 1979 (Cth).
72–13	Section 285 of the Telecommunications Act 1997 (Cth) should be amended to provide that a disclosure of an unlisted number is permitted if the disclosure is made to another person for purposes connected with dealing with the matter or matters raised by a call to an emergency service number.
72–14	The Australian Government should amend s 285(3) of the Telecommunications Act 1997 (Cth) to provide that before the Minister specifies a kind of research for the purpose of the use or disclosure of information or a document contained in the Integrated Public Number Database, the Minister must be satisfied that the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the Telecommunications Act to the information in the Integrated Public Number Database.
72–15	The Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1) should be amended to provide that an authorisation under the integrated public number database scheme is subject to a condition requiring the holder of the authorisation to notify the Privacy Commissioner, as soon as practicable after becoming aware: (a) of a substantive or systemic breach of security that reasonably could be regarded as having an adverse impact on the integrity and confidentiality of protected information; and (b) that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.
72–16	The Telecommunications Act 1997 (Cth) should be amended to provide that directory products that are produced from data sources other than the Integrated Public Number Database should be subject to the same rules under Part 13 of the Telecommunications Act as directory products which are produced from data sourced from the Integrated Public Number Database.
72–17	The Telecommunications Act 1997 (Cth) should be amended to prohibit the charging of a fee for an unlisted (silent) number on a public number directory.

73. Other Telecommunications Privacy Issues	
73–1	Section 79 of the Telecommunications (Interception and Access) Act 1979 (Cth) should be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, in the possession of an agency, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.
73–2	Section 79 of the Telecommunications (Interception and Access) Act 1979 (Cth) should be amended to require the destruction of nonmaterial content intercepted under a B-Party warrant.
73–3	The Telecommunications (Interception and Access) Act 1979 (Cth) should be amended to provide that the Australian Security Intelligence Organisation and enforcement agencies must destroy in a timely manner irrelevant material containing accessed telecommunications data which is no longer needed for a permitted purpose.
73–4	Sections 151 and 163 of the Telecommunications (Interception and Access) Act 1979 (Cth) should be amended to provide for reporting requirements relating to the use of stored communication warrants that are equivalent to the interception warrant reporting requirements under Part 2–7 and section 102 of the Act.
73–5	The Australian Government Attorney-General's Department should develop and, where appropriate, publish guidance on the interception and access of information under the Telecommunications (Interception and Access) Act 1979 (Cth), that addresses: (a) the definition of the term 'telecommunications data'; (b) when voluntary disclosure of telecommunications data to the Australian Security Intelligence Organisation and other enforcement agencies is permitted; and (c) timeframes within which agencies should review holdings of information and destroy information.
73–6	The Telecommunications (Interception and Access) Act 1979 (Cth) should be amended to provide expressly that where the Ombudsman has reason to believe that an officer of an agency is able to give information relevant to an inspection of the agency's records relating to access to a stored communication, the Ombudsman may: (a) require the officer to give the information to the Ombudsman and to attend a specified place in order to answer questions relevant to the inspection; and (b) where the Ombudsman does not know the officer's identity, require the chief officer, or a person nominated by the chief officer, to answer questions relevant to the inspection.
73–7	The Australian Communications and Media Authority should add the Office of the Privacy Commissioner as a member of the Law Enforcement Advisory Committee.
73–8	The Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority should develop memorandums of

	understanding, addressing: (a) the roles and functions of each of the bodies under the Telecommunications Act 1997 (Cth), Spam Act 2003 (Cth), Do Not Call Register Act 2006 (Cth) and Privacy Act; (b) the exchange of relevant information and expertise between the bodies; and (c) when a matter should be referred to, or received from, the bodies.
73–9	The document setting out the Office of the Privacy Commissioner's complaint-handling policies and procedures (see Recommendation 49–8), and its enforcement guidelines (see Recommendation 50–3) should address: (a) the roles and functions of the Office of the Privacy Commissioner, Telecommunications Industry Ombudsman and the Australian Communications and Media Authority under the Telecommunications Act 1997 (Cth), Spam Act 2003 (Cth), Do Not Call Register Act 2006 (Cth) and Privacy Act; and (b) when a matter will be referred to, or received from, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority.
73–10	The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish guidance relating to privacy in the telecommunications industry. The guidance should: (a) outline the interaction between the Privacy Act, Telecommunications Act 1997 (Cth), Spam Act 2003 (Cth) and Do Not Call Register Act 2006 (Cth); (b) provide advice on the exceptions under Part 13 of the Telecommunications Act, Spam Act and the Do Not Call Register Act; and (c) outline what is required to obtain an individual's consent for the purposes of the Privacy Act, Telecommunications Act, Spam Act and Do Not Call Register Act. This guidance should cover consent as it applies in various contexts, and include advice on when it is, and is not, appropriate to use the mechanism of 'bundled consent'.
73–11	The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish educational material that addresses the: (a) rules regulating privacy in the telecommunications industry; and (b) various bodies that are able to deal with a telecommunications privacy complaint, and how to make a complaint to those bodies.

*
**