Australian Government
Attorney-General's Department

Departmental submission

Inquiry into the comprehensive revision of the *Telecommunications (Interception and Access) Act 1979*

Senate Legal and Constitutional Affairs References Committee

Contents

Introduction

The *Telecommunications (Interception and Access) Act 1979* (TIA Act) has two key objectives. First, the Act protects the privacy of telecommunications by criminalising intercepting or accessing communications. Confidence in the privacy of their communications allows people to use communications technologies to their full potential. Without an assurance of privacy, people would be reluctant to have personal conversations over the telephone or conduct transactions over the Internet. Communications privacy is becoming more important as more aspects of life move online.

Second, the TIA Act enables Australia's law enforcement, anti-corruption and national security agencies to investigate serious wrongdoing. The Act allows these agencies to apply for warrants to intercept communications when investigating serious crimes and threats to national security. Interception warrants are powerful tools because they provide agencies with immediate, first-hand information about what a person of interest is doing or saying. The Act also allows agencies to access telecommunications data, which is a key investigative tool used in almost every significant law enforcement and national security investigation.

The interception regime contains robust safeguards, oversight and accountability measures to ensure that agencies use the powers under the Act lawfully. Agencies must obtain an independently-issued warrant to access communications, and access to telecommunications data is permitted only where it is reasonably necessary and proportionate for a particular investigation. The Act then limits how agencies may use information they have lawfully obtained. Finally, the Act requires that law enforcement agencies are subject to independent oversight to ensure that agencies respect these limits. The Australian Security Intelligence Organisation (ASIO) is subject to oversight by the Inspector-General of Intelligence and Security (IGIS) under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act).

With the development of communications technology, however, the Act is in danger of no longer sufficiently fulfilling either of its key objectives and its oversight arrangements are, in part, fragmented and incomplete. The privacy protections in the Act, although strong, require future-proofing to keep pace with the changes in technology. Similarly, the lawful access regime has not fully adapted to the use of modern communications technologies by serious criminals, organised criminal groups, terrorist networks and foreign intelligence services.

Therefore, the Department supports the comprehensive revision of the TIA Act and welcomes this inquiry, which follows previous recommendations of the Australian Law Reform Commission (ALRC),[1] and the Parliamentary Joint Committee on Intelligence and Security (PJCIS)[2] to review and comprehensively revise the TIA Act.

This submission is divided into two parts. Part 1 provides an overview of the TIA Act, including its role in protecting the privacy of Australians' telecommunications and how telecommunications interception is used in law enforcement and national security investigations. Part 2 contains policy and technical analysis about the key drivers and priorities for the revision of the Act.

This submission reflects the preliminary views of the Department. 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. Additionally, due to the timing of this inquiry, the Department has not had the opportunity to engage with interested stakeholders, as recommended by the PJCIS. Summaries of the Department's preliminary views on the recommendations made by the PJCIS and ALRC are at **Attachment A** and **Attachment B**, respectively.

---

[1] ALRC, *For your information: Australian Privacy Law and Practice*, Report No 108 (2008) Recommendation 71-2.

[2] PJCIS, Parliament of Australia, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Recommendation 18.

Part I: The Purpose of the TIA Act

The TIA Act has two key objectives. First, the Act protects the privacy of telecommunications by criminalising intercepting or accessing communications. Second, the Act enables Australia's law enforcement, anti-corruption and national security agencies to investigate serious wrongdoing. The Act also contains a series of safeguards, oversight and accountability measures to ensure that agencies use the powers under the Act lawfully.

Protecting the privacy of communications

It is vital that people have confidence in the privacy of their communications. Modern technologies have revolutionised the ability of people to communicate, collaborate and express themselves. Strong legal protections underpin public confidence in the privacy of their communications and are essential to allow people to use these technologies to their full advantage, such as by having personal conversations, engaging in political speech, conducting banking and buying and selling goods online.

As such, the TIA Act and the *Telecommunications Act 1997* (Telecommunications Act) establish broad and powerful protections for the privacy of telecommunications. These protections go well beyond the protections afforded to many other kinds of personal and sensitive information in Australia, such as the protections offered by the *Privacy Act 1988*. In particular, the Act criminalises unlawful access to communications and allows people to seek civil remedies for unlawful breaches of the privacy of their communications.

The privacy framework established by the TIA Act was, however, conceived in another era. In 1979, the communications environment was typically limited to home and office telephones connected by copper wires provided by a single Government-owned carrier. The Australian Media and Communications Authority's (ACMA) *Communications Report 2012–13* highlights how far Australia's communication environment has evolved:[3]

- 14.24 million people had access to the internet in the home at June 2013, an increase of two per cent since June 2012
- 7.50 million people used the internet via their mobile phone during June 2013, a 33 per cent increase over the number of mobile internet users during June 2012
- Australians are more intensive users of the internet noting that there was a 59 per cent increase in internet downloads during the June quarter 2013 compared to the June quarter of 2012
- revenue from the sale of goods or services online by businesses operating in Australia reached $237 billion during 2011–12, a 25 per cent increase over 2010–11, and
- more Australians are transacting online with 12.86 million people using the internet for banking or paying bills and 10.44 million buying or selling goods or services online in the six months to May 2013, a 10 per cent and 9 per cent increase respectively over the six months to May 2012.

The trend of Australians communicating more intensively and conducting more of their lives online, reinforces the need to ensure that the privacy of Australian telecommunications is strongly protected.

---

[3] ACMA, *Communications Report 2012–13* (2013) 3-4.

However, the advent of social media, smartphones and tablets, GPS and location tracking and the proliferation of communications providers and applications, have given rise to new challenges to the framework. It is essential that the privacy protections enshrined in the TIA Act adapt to the evolving communications environment.

Access to communications by law enforcement and anti-corruption agencies

Two of Government's highest duties are protecting the safety and security of Australians and upholding the rule of law. Australia's law enforcement and anti-corruption agencies play central roles in fulfilling these duties, but cannot do so without the appropriate tools.

Serious criminals and organised criminal groups make extensive use of communications technologies to plan and carry out crimes. Outlaw motorcycle gangs and drug cartels use encrypted communications and sophisticated tradecraft to communicate with specialist money launderers in foreign countries. Child exploitation rings hide their activities by setting up secure file-sharing networks from inside the comfort of their homes. Terrorists in Australia use the internet to plan attacks and receive training from international terrorist groups.[4] Corrupt public officials use phone calls, emails and text messages to abuse their positions of trust.[5]

The ability to access communications and telecommunications data is, therefore, not just useful for Australia's law enforcement and anti-corruption agencies. These powers are essential to allow agencies to investigate a wide range of the most serious and sophisticated criminal threats in this country. The Department's view on this issue is consistent with that of a number of international organisations, including the United Nations Office on Drugs and Crime (UNODC), which states:[6]

> *The value of employing electronic surveillance in the investigation of some forms of serious crime, in particular organized crime, is unquestionable. It allows the gathering of information unattainable through other means.*

The United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) has provided a more detailed explanation of the value of lawful access to communications to law enforcement agencies:[7]

> *Electronic surveillance represents the single most important law enforcement weapon against organized crime. There is nothing as effective as proving a crime through the defendant's own words. Its evidence provides reliable, objective evidence of crimes through the statements of the participants themselves.*
>
> *Additionally, electronic surveillance enables law enforcement agencies to learn of conspirators' plans to commit crimes before they are carried out. This allows them to survey the criminal activities, such as delivery of contraband and conspiratorial meetings, or to disrupt and abort the criminal activities, where appropriate, making electronic surveillance particularly helpful in preventing the occurrence of violent crimes*

Organised criminal groups are a major focus of Australian law enforcement agencies' use of powers under the TIA Act. In 2012-13, more than half of all interception warrants issued to law enforcement agencies were for organised crime, drug trafficking and serious drug or money

---

[4] Department of Foreign Affairs and Trade, *Transnational Terrorism: The Threat to Australia* (2004) 17.
[5] For example: Operation Ivanhoe: http://www.cdpp.gov.au/case-reports/joseph-harb-and-paul-john-katralis.
[6] UNODC, *Current practices in electronic surveillance in the investigation of serious organized crime* (2009) 1.
[7] UNAFEI, 'Special Investigative Tools to Combat Transnational Organized Crime (TOC)', 58 *Resource Material Series* 228, 235-36.

laundering offences.[8] The use of such powers to combat organised criminal activity is consistent with international best practice. For example, in 2012, the Financial Action Task Force (FATF)[9] issued the FATF Recommendations, setting out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Recommendation 31 (Powers of law enforcement and investigative authorities) states, *inter alia*, that:[10]

> *Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery.*

The tools available under the interception regime are often the only investigative techniques capable of identifying and disrupting organised criminal activities. More 'traditional' methods of investigation, such as physical surveillance or the use of informants or undercover agents not only pose significant risks to operational security, they also place officers and agents at risk. As UNAFEI has noted:[11]

> *The use of traditional investigative methods to combat TOC [transnational organised crime] has proved to be very difficult and ineffective. This state of affairs therefore calls for the use of special investigative tools such as controlled delivery, undercover operations and electronic surveillance (wiretapping, communications interception etc) by law enforcement agencies to effectively control TOC.*

The power to lawfully access communications and telecommunications data allows agencies to gather unique intelligence and evidence from inside criminal organisations and networks about their structure, plans and activities, as well as their co-conspirators and criminal associates, without being detected.

Obtaining and sharing lawfully accessed communications with other countries via the mutual assistance process is also a critical part of the regime, given the globalisation of telecommunications. Mutual assistance allows agencies to share evidence for the investigation and prosecution of transnational crime, particularly drug trafficking, fraud, money laundering, child exploitation offences and terrorism offences. In a trend consistent with the past five years, Australia saw an increase in the number of requests made by Australia to foreign countries for mutual assistance in criminal matters.[12]

The focus of Australia's law enforcement agencies on organised crime reflects the serious harm it inflicts on Australian society. The ACC estimates that organised criminal activity costs Australia $15bn each year.[13] Organised crime not only has a direct impact on individuals, but also has

---

[8] Attorney-General's Department, *TIA Act Annual Report 2012-13* (2013), 19.

[9] FATF is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. FATF's mandate is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

[10] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations* (2012) 25.

[11] Above n 7, 228.

[12] Above n 8, Appendix 6.

[13] ACC, *Organised Crime in Australia 2013* (2013) 6.

broader social, economic and governance implications. Australia's national security strategy lists serious and organised crime as a key national security risk,[14] and explains that:[15]

> *Serious and organised crime can undermine our border integrity and security. It can erode confidence in institutions and law enforcement agencies, and damage our economic prosperity and regional stability. It can involve the procurement, distribution and use of illegal weapons. This type of crime is highly adaptive and may link to, or exacerbate, other significant issues of national security, such as terrorism and malicious cyber activity.*

Australian law enforcement agencies also use their powers under the TIA Act to investigate serious criminals that are not part of organised criminal groups, such as murderers, rapists and kidnappers.

Serious criminal investigations are often complex. Agencies are generally trying to solve crimes that have already happened, or are attempting to investigate crimes that are in progress. Valuable information and evidence is constantly at risk of being lost with the passage of time. Serious offenders are often unwilling to cooperate, meaning that agencies possess only fragments of the evidence required to investigate and prosecute their crimes.

Telecommunications data is often used at the early stages of investigations to build a picture of a target and their network of associates. Agencies, by definition, begin their investigations several steps behind. Agencies use lawfully accessed communications and telecommunications data to fill in these gaps. The ability to reconstruct events leading up to and surrounding a crime allows agencies to rapidly determine the size and scope of an investigation—for example, who is a person of interest, whether the target is a lone actor or part of an extended criminal conspiracy, or whether a new target has links to known criminal or terrorist groups.

Lawful access to telecommunications data allows agencies to obtain crucial information and evidence that often could not be obtained in any other way. In particular, alternative methods, such as surveillance, cannot provide essential historical information required in criminal investigations.

By way of illustration, the Victoria Police recently conducted a highly-publicised investigation into the disappearance and suspected murder of a woman in Melbourne, which relied heavily upon lawful access to telecommunications data.

Investigators established that the victim's mobile phone service was provided by Vodafone. Victoria Police were then able to trace the final movements of the victim's mobile phone through telecommunications data generated by Vodafone's Visitor Location Register (VLR).

A person of interest was soon identified, and it was established that his mobile phone also utilised the Vodafone network. Telecommunications data generated by the VLR on this person's mobile phone was compared to that of the victim's, and it showed a striking similarity in the location and movement of both mobile phones over a period of time. This information was invaluable to investigators as it enabled them to focus their investigation on this particular individual who had no previous connection with the victim.

The suspect was subsequently arrested and charged with murder. After a plea of guilty, the offender was convicted and sentenced to 35 years imprisonment.

Finally, law enforcement agencies use their powers under the TIA Act as a means to protect and promote public confidence in communications technology and online services. Information and communications technology is an integral part of modern life. Whether people have a computer at

---

[14] Department of Prime Minister and Cabinet, *Strong and secure: A Strategy for Australia's National Security* (2013) ii.
[15] Ibid, 11.

home, use online banking services or simply receive electricity supplies, the community's reliance on technology is increasing. Government and business also take advantage of opportunities for economic development through increased use of information technology and a technology aware population with internet connections locally and overseas.

Serious and complex cybercrimes—such as large scale breaches involving personal, business and/or financial information, breaches of major computer systems used by Australian businesses, sophisticated online fraud and scams, and crime which directly impacts the banking and finance sector—have the potential to erode public faith in these technologies and services.

Cybercrime, by definition, has a limited physical footprint. For online investigations, telecommunications data and content is, in many cases, the primary form of information used by law enforcement agencies to identify, investigate, prevent and prosecute cybercrimes. For example, telecommunications data is critical for tracing cyber-attacks across networks and, in particular, for linking an Internet Protocol (IP) address back to a real-world offender.

The powers to lawfully access communications and telecommunications data are some of the most effective tools that Parliament has granted these agencies. Communications lawfully accessed under the TIA Act were used in more than 3,000 arrests and 2,765 convictions in the 12 months to June 2013.[16] This equates to more than one conviction for every two warrants issued.[17]

These figures likely underestimate the effectiveness of interception. Lawfully accessed information can often assist agencies to obtain a conviction without being entered into evidence. For example criminals regularly enter guilty pleas after being shown lawfully accessed communications demonstrating their guilt. Additionally, lawfully accessed information—in particular telecommunications data—may provide a crucial lead for an investigation, even if the information is not itself used in the final prosecution.

Access to communications by ASIO

ASIO is Australia's national security intelligence service. ASIO is charged with identifying and investigating threats to Australia's security and providing advice to government to protect Australia, its people and its interests. Those threats include espionage, sabotage, politically motivated violence including terrorism, the promotion of communal violence and acts of foreign interference.

Under the TIA Act, ASIO may apply to the Attorney-General for interception warrants to investigate activities prejudicial to security or to collect foreign intelligence.

The Australian security environment in 2014 continues the trend of shifting threats. Terrorism remains the most immediate threat to Australian security and interests; however other threats have gained momentum.[18]

Telecommunications interception plays a key role in almost every counter-terrorism investigation, providing critical intelligence and evidence to allow ASIO and law enforcement agencies to disrupt terrorist attack plans and prosecute those seeking to undertake mass casualty attacks. Since 2001, intercepted information from Australian agencies has contributed to the disruption of at least four planned terror attacks in Australia and the conviction of 22 people on terrorism offences under the *Criminal Code Act 1995*.

Instances of espionage and foreign interference within Australia have continued to increase, both in terms of the number of occurrences and the range of actors.[19] In particular, the scale and

[16] Above n 8, 12, 38.
[17] A total of 4,793 warrants were issued in 2012-13, for an average of 0.58 convictions per warrant.
[18] ASIO, *ASIO Report to Parliament 2012-2013* (2013), vii.

sophistication of cyber-espionage conducted against Australian Government and private sector systems has increased significantly in recent years.[20] The potential harm to Australia from these activities extends from traditional national security, defence and foreign policy issues through to private sector intellectual property, commercial secrets and strategies, science and technology data, and economic information.

ASIO advises that the rapidly changing technological environment poses real challenges to its efforts to identify and respond to attempts at attacking or infiltrating systems holding sensitive information.[21] As the actors involved undertake this activity in 'cyberspace', the lawful interception of their communications is often a crucial aspect of counter-espionage investigations.[22]

[19] Ibid.
[20] Ibid, 5.
[21] Ibid.
[22] Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper (2012) 15.

Part II: The need to comprehensively revise the TIA Act

The advance of communications technologies over the 35 years following the creation of the TIA Act has greatly benefitted Australia and the world. However, these technological developments also pose challenges to the privacy and lawful access regimes established by the Act.

Since its enactment in 1979, the TIA Act has been frequently amended to address changes in telecommunications, law enforcement and national security environments. A list of the amendments to the Act since 2000 and a brief explanation of the reason for each amendment is at **Attachment E**. The revolution in communications technology poses a range of challenges to the TIA Act, including:

- exposing Australians to new privacy challenges that will require reconsideration of the key assumptions on which the existing privacy framework is based
- providing criminals, terrorists and others who threaten national security with new and sophisticated ways to communicate and organise without being identified, investigated or prosecuted, and
- challenging traditional jurisdictional approaches to industry regulation and engagement.

Australia's law enforcement and security capabilities must stay ahead of the techniques and technologies used by organised criminals, terrorists and foreign intelligence services that endanger our national security and interests, and the safety of our citizens. Changes in communications technologies often require Australia's agencies to adapt and find new ways of gathering evidence and intelligence.

Recent changes in the communications environment have, however, been more dramatic and challenge the underlying legislative framework within which Australia's law enforcement and national security agencies function. A legislative response is required to avoid the degradation of these agencies' investigative capabilities. Without such a response, the ability of Australia's governments to fulfil their core duties to protect the safety and security of Australians and upholding the rule of law would be compromised.

Australia is not alone in facing the challenge of interception legislation being made obsolete by changing technology and behaviour. The communications environment is globalised, and technologies made available in one country are rapidly adopted around the world. Similarly, techniques used by serious criminals and terrorists to thwart investigations in one country rapidly spread to others. For example, in February 2011, the US Federal Bureau of Investigation described the growing gap between their legal authority and technical capability driven by technological change, as 'going dark'.[23] As such, understanding and engaging with the international environment is both more relevant than ever.

Governments around the world have identified the need to modernise their lawful access frameworks, consistent with the findings of the PJCIS that changes in the global telecommunications environment are degrading agencies investigative capabilities.[24] International developments grant Australia the opportunity to learn from other countries' experiences and act consistently with international trends.

---

[23] Evidence to the House Judiciary Committee Subcommittee on Crime, Terrorism, and Homeland Security, United States Congress, 17 February 2011, (Ms Valerie Caproni, General Counsel, Federal Bureau of Investigation).

[24] Above n. 2, paragraphs 2.67, 2.68 and 2.76.

Examples of recent overseas actions include:

- In June 2011, the Japanese Parliament, the Diet, passed legislation modernising its Criminal Procedure Law to allow agencies to combat communications and technology-enabled crime
- In November 2013, the New Zealand Parliament passed the *Telecommunications (Interception Capability and Security) Act 2013*, modernising its laws for lawful access to communications and introducing a framework to ensure the security of its networks, and
- In December, 2013, the French Parliament enacted the *Loi de Programmation Militaire* (the Military Program Law, or LPM). The LPM includes provisions permitting law enforcement and national security agencies to obtain telecommunications data under an authorisation.

Whilst differing legal systems and legislative frameworks mean that no foreign law can be simply adopted in Australia, the international context is highly relevant. International inquiries and reviews have identified the same challenges as are identified in this submission. The Department's assessment is that no substantive issue facing the privacy and lawful access frameworks under the TIA Act is unique to Australia and no policy solution considered in Australia has not been considered or implemented overseas. As such, the developments in the international environment have informed the Department's preliminary views as outlined in this submission.

Reform of the privacy framework

The privacy regime established by the Telecommunications Act and TIA Act contains powerful protections for the privacy of telecommunications and the associated data. These protections go well beyond the protections afforded to many other kinds of personal and sensitive information in Australia, such as the protections offered by the *Privacy Act 1988*.

The regulation of lawful access to communications in Australia does not occur in a vacuum. Australia's international legal obligations are highly relevant. The right to privacy is frequently referred to in this context. The TIA Act contains substantial controls and safeguards around the lawful access to communications by law enforcement, anti-corruption and national security agencies aimed at ensuring that lawful access respects the privacy of Australians and is proportionate to the investigative need. These protections, controls and safeguards comply with international law, including:

- Articles 17 of the International Covenant on Civil and Political Rights (ICCPR), which provides that no one shall be subjected to arbitrary or unlawful interference with their privacy or correspondence, and that everyone has the right to the protection of the law against such interference
- Article 19 of the ICCPR, which provides that everyone shall have the right to hold opinions without interference, and the right to freedom of expression subject only to such restrictions as are provided by law and are necessary for respect of the rights and reputations of others, or for the protection of national security, public order or of public health or morals
- Article 12 of the Universal Declaration of Human Rights, which provides that no one shall be subjected to arbitrary interference with his privacy and that everyone has the right to the protection of the law against such interference, and
- Article 15 of the Council of Europe Convention on Cybercrime, which requires that the application of powers and procedures are subject to conditions and safeguards which shall provide for the adequate protection of human rights and liberties, and which shall incorporate the principle of proportionality.

The TIA Act protects privacy and freedom of expression by criminalising the interception of the content of communications and by establishing a civil remedies regime entitling any person whose communications have been unlawfully accessed to seek recompense.

The Telecommunications Act also prohibits a range of people associated with the telecommunications industry, such as employees of carriers and emergency call service people, from disclosing any information or document relating to a communication, which includes telecommunications data.

Australia's law enforcement, anti-corruption and national security agencies may only access communications and telecommunications data for proper purposes under a warrant or authorisation, which include the consideration of proportionality in all cases. The use of these powers is also subject to a range of safeguards, including internal compliance frameworks and independent oversight, ensuring that lawful access to telecommunications is not arbitrary or unlawful.

The revolution in communications technologies has given rise to a range of new challenges and is changing community expectations about privacy. The Department's view is that the privacy protection framework established by the TIA Act remains robust overall, but is under increasing pressure in several areas, including that:

- communications passing 'live' over the network are protected in different ways and to differing degrees to communications 'stored' by service providers, based on outdated assumptions about their respective privacy sensitivity
- the privacy protections should be future-proofed to account for new communications technologies, industry structures or broader technological developments that will have privacy implications, and
- the relevant provisions are distributed between parts of the TIA Act and the Telecommunications Act, making it difficult to clearly understand how the privacy of telecommunications is protected.

The Department agrees with the ALRC's assessment that telecommunications contain particularly privacy sensitive information justifying special protections.[25] As such, the Department considers that a reformed TIA Act should maintain the privacy protections currently afforded to the content of telecommunications and continue to permit people whose privacy of telecommunications is infringed to seek recompense under the Act.

The Department further considers that the reform of the TIA Act represents an opportunity to future-proof the existing privacy framework to account for technological change. The Department's preliminary view is that there are, in particular, opportunities to modernise the protections afforded to stored communications and telecommunications data. Additionally, any review should acknowledge that technological evolution means that threats to privacy will come from an ever wider range of sources and should be responsive to emerging threats to communications privacy.

Modernisation and reform in each of these areas is consistent with PJCIS Recommendation 18.

[25] Above n 1, paragraphs 71.49 to 71. 56..

Strengthening the protections afforded to stored communications

The TIA Act protects the privacy of stored communications held by 'carriers' and 'carriage service providers', as defined under the Telecommunications Act.[26]

Significant technological changes within the telecommunications industry are driving the emergence of a new class of service providers, known as 'ancillary service providers'. These are companies that deliver their services 'over the top' of carrier and carriage service provider infrastructure, such as social media and webmail providers, and that play a major role in the Australian telecommunications market.

Consistent with PJCIS Recommendation 14, the Department's preliminary view is that, to the extent that ancillary service providers are within Australia's jurisdiction—many are located offshore but supply services inside Australia—a reformed TIA Act should clearly protect the privacy of communications held by these providers.

Consolidating and strengthening protections afforded to telecommunications data

The ALRC has previously identified that telecommunications data can contain particularly sensitive personal information justifying special legal protection. [27] The Law Council of Australia has expressed similar views. [28] The Department agrees with these views, which are consistent with the current, higher protections afforded to telecommunications data under the Telecommunications Act and TIA Act compared with other types of personal and sensitive information.

However, the Department's view is that the current privacy framework for telecommunications data is, in part, fragmented. The ALRC has identified the issue of the fragmentation of the protections afforded to telecommunications data. [29] The Department is concerned that this fragmentation may pose a barrier to public understanding of the privacy regime and may, therefore, undermine public confidence in the privacy of this information.

Moreover, the ALRC has further identified that modern business models based on collecting telecommunications data—in some cases without people's knowledge—are challenging the effectiveness of the existing privacy frameworks, [30] and has suggested that the regulation of telecommunications data be reviewed. [31]

The Department is conscious that the innovative collection, analysis and use of telecommunications information by the private sector has yielded significant benefits to society. These range from free online communications and networking services funded by targeted advertising to more efficiently designed and organised department stores and supermarkets made possible by companies tracking the locations, purchases and habits of customers.

As such, the Department's preliminary view is that there may be merit in exploring options to improve privacy protection in this area. Any such exploration should be undertaken in close consultation with key stakeholders and interested parties to avoid creating unintended consequences for the telecommunications industry or imposing undue burdens on businesses developing and implementing innovative, information-based products and services.

---

[26] TIA Act, s 108.
[27] Above n 1, paragraphs 71.49 to 71. 56.
[28] Law Council of Australia, Submission no 96 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms to Australia's National Security Legislation*, 20 August 2012, paragraph 168.
[29] Above n 1, paragraphs 71.52 and 71.54.
[30] ALRC, *Serious Invasions of Privacy in the Digital Era*, Issues Paper 43 (2013) paragraph 164.
[31] Ibid, paragraph 176.

Preserving the capability of agencies to investigate serious crime and safeguard security

Organised criminal groups, terrorist networks and foreign intelligence services exploit communications technologies to plan and commit serious crimes and to compromise the safety and security of Australia. Lawful access to communications is, therefore, a vital and effective tool for Australia's law enforcement, anti-corruption and national security agencies, whose work makes Australia, and our region, a safer and more secure place.

Despite the importance of lawful interception and access, and the best efforts of Government to maintain the TIA Act, the lawful access regime is no longer adequate. In particular, it no longer effectively allows Australia's law enforcement, anti-corruption and national security agencies to:

- reliably identify communications that are to be lawfully accessed as they pass over the telecommunication network
- if identified, consistently obtain those communications and the associated telecommunications data
- once lawfully accessed, effectively interpret the communications to extract valuable evidence or intelligence about serious criminal activity or threats to national security, and
- once properly analysed, appropriately act on and utilise the intelligence and evidence gathered through lawful interception.

In evidence to the PJCIS, Commissioner Scipione of the New South Wales Police Service summarised the challenges facing Australia's law enforcement and national security communities:[32]

> *A further significant challenge for law enforcement agencies investigating national security and serious criminal matters is the increasing use of sophisticated technologies by criminals. Frankly, organised criminals are now able to operate outside the reach of ordinary telecommunications interception and law enforcement agencies that are dealing with criminals who have access to unprecedented advancements in technology. Legislation that not only fails to adequately recognise this but significantly fails to future proof itself against rapidly emerging technologies is what we are dealing with here.*

The PJCIS acknowledged that rapid change in the telecommunications environment is degrading the ability of Australian agencies to lawfully access communications.[33]

A more sophisticated and flexible approach to lawful access and inter-agency collaboration is required, backed by strong safeguards and independent oversight. Comprehensively revising the TIA Act would allow Parliament to ensure that Australia's law enforcement, anti-corruption and national security agencies are able to operate in a more complex communications and operational environment.

Revising the TIA Act would also allow for amendments, consistent with the PJCIS's recommendations, to ensure that the powers available to agencies remain proportional. These include standardising the thresholds for access to the content of communications, as well as limiting access to and strengthening independent oversight of lawful access to traffic data.

---

[32] Evidence to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 26 September 2012, 18 (Andrew Scipione APM, Commissioner, NSW Police Service).
[33] Above n 2, paragraphs 2.67, 2.68 and 2.76.

Reforming access to the content of telecommunications

Lawful access to the content of telecommunications is an extremely successful, low-risk, cost-effective and timely tool for law enforcement, anti-corruption and national security agencies to obtain intelligence and evidence. Rapid and significant technological change is degrading this key capability.

When the TIA Act was enacted, agencies and Parliament could legitimately expect that most, if not all of a person of interest's communications could be lawfully accessed under a warrant. Significant changes in communications technology mean that today, this expectation is far lower, representing a significant gap between agencies' apparent lawful authority and their real-world capability. Adapting the lawful access regime to the modern telecommunications environment is a vital first step in arresting the decline in agencies' investigative capabilities.

The core problem facing the lawful access regime under the TIA Act is that the regime does not reflect the complexity of the modern communications environment. Instead, it assumes that:

- communications to be intercepted are easily identified
- a stream of traffic to be intercepted can be isolated from the rest of the communications passing over the network
- carriers and carriage service providers (telecommunications companies and internet service providers) control the traffic passing over their networks
- carriers and carriage service providers are the only entities which control public telecommunications networks
- intercepted communications are easily interpreted or understood, and
- there are reliable sources of associated communications data that link people with identifiers and identifiers to communications.

These assumptions mean the TIA Act takes a technical approach to lawful access which was appropriate to the prevailing technologies of the 1960s and 1970s but, with the rise IP communications, now fails to recognise the particular demands created by a diverse telecommunications sector.

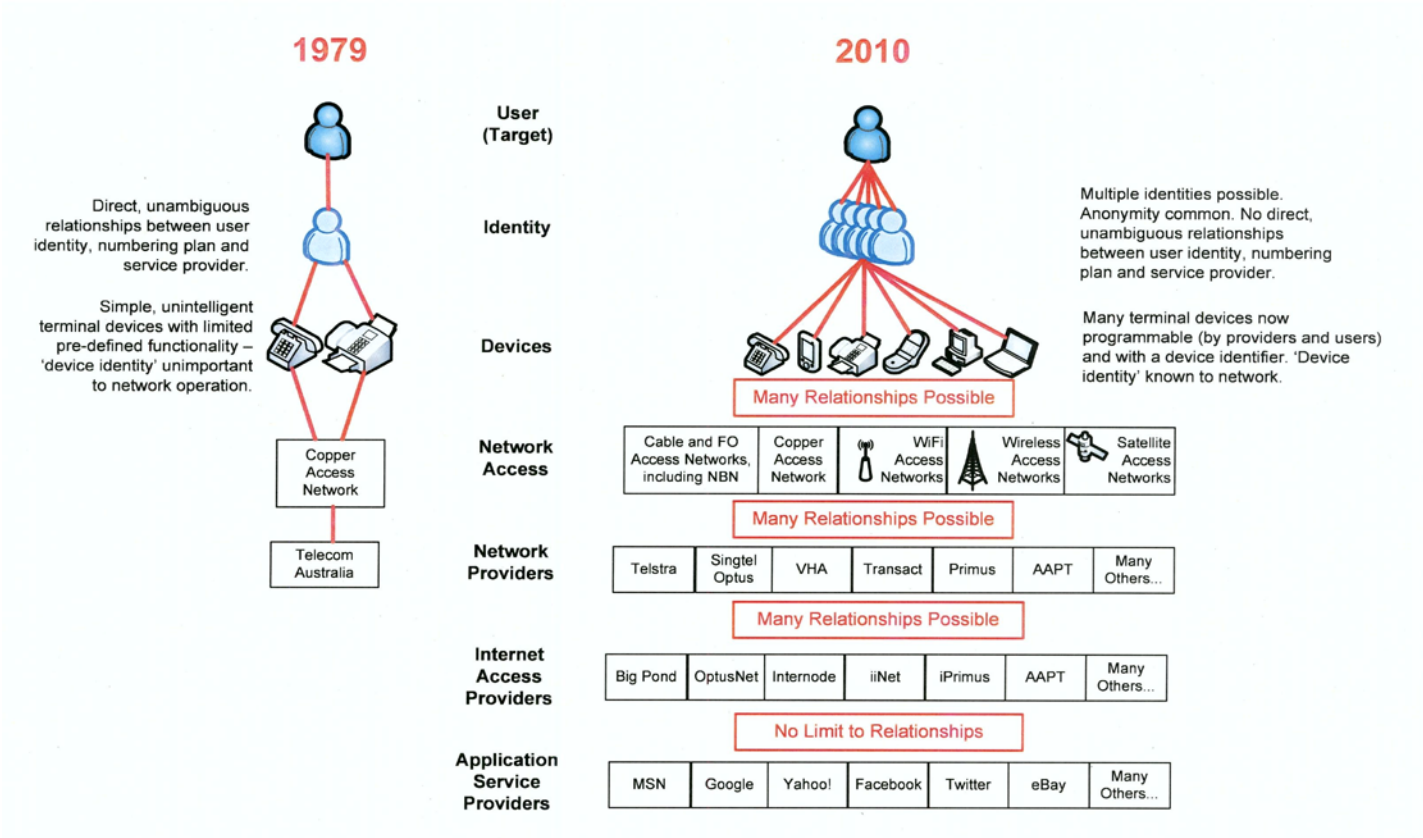

Figure 1: Diagrammatic example of the services and devices available in 1979 compared to 2010.

The Department considers that a revised TIA Act should continue to permit a strictly limited number of agencies to access the content of communications under warrant.

To preserve the capabilities of agencies, the Department's preliminary views are that:

- the warrant regime should be simplified to involve a single warrant that authorises lawful access to a person of interest's communications, consistent with PJCIS Recommendation 6
- the Act should adopt a more targeted, 'attribute-based' model for access to communications, consistent with PJCIS Recommendation 7
- an authorised warrant should provide agencies with the ability to vary the attributes of the communications to be lawfully accessed under a warrant, subject to safeguards, consistent with PJCIS Recommendation 7
- issuing authorities should be able to authorise an agency to issue 'intelligibility assistance notices', requiring a person to provide information or assistance to place previously lawfully accessed communications into an intelligible form, as discussed by the PJCIS at Recommendation 16, and
- the industry assistance framework under a reformed Act should be reviewed to ensure that it remains fit-for-purpose and appropriate in the modern telecommunications environment, as discussed below.

Simplifying the warrant regime

The TIA Act contains four warrant regimes for lawful access to the content of communications by law enforcement and anti-corruption agencies. Three of these warrants relate to access to 'live' communications, and the fourth relates to access to 'stored' communications held by carriers.

The distinction between access to live and stored communications currently embodied in the TIA Act is based on an assumption that stored communications were generally more 'considered' and so less privacy sensitive. The Department considers that changing communications technologies and habits have undermined this rationale.

The Department's preliminary view is that there may be merit in standardising the thresholds for access to the content of communications, consistent with PJCIS Recommendation 6, having regard to 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.

Attribute-based interception

Currently, warrants issued under the TIA Act may only authorise the interception of 'services' or 'devices'—such as a particular internet connection or telephone. The service or device identifiers are the technical means that the telecommunications industry uses to identify the communications for retrieval under a warrant. This approach is technologically-specific and reflects historic assumptions about how telecommunications operate. The diversification of the telecommunications industry, changing communications habits and changes to the technical operation of modern telecommunications networks mean that new ways of identifying communications are both available and required.

Without reform, technological change will make the current, service and device-based provisions obsolete. In the Department's view, a more targeted and technologically-neutral approach is required to address this challenge. The Law Council of Australia has previously argued that: [34]

> *[T]he dramatic and rapid advances in technology have had a transforming impact on telecommunications in Australia and around the world, and that this in turn justifies a careful review of the adequacy of the current telecommunication interception regime. However, it does not follow that the challenges posed by technological advances must always be met by an expansion in interception or access capabilities. It may be, for example, that a more targeted approach to accessing communications or data is needed in light of the exponential increase in the generation of communications and data by the community, rather than a power that would allow a broader range of communications or data to be accessed or retained.*

Consistent with PJCIS Recommendation 7, the Department's preliminary view is that there may be merit in implementing a technologically-neutral, 'attribute-based' warrant regime.

---

[34] Above n 28, paragraph 74.

Under this approach, a warrant would continue to authorise access to a particular person's communications, but would describe the communications that the service provider is to access and provide to the agency by using a combination of technical features or 'attributes'—rather than just a service or device identifier. Those attributes could include a specific account, a time of day, a geographic location or a technical feature of the communication.

The use of attributes would allow warrants to be more targeted and more effective. By way of illustration, suppose a criminal sends emails from a webmail account to a range of criminal associates each night at 11pm, using their family's internet connection. Currently, a warrant would specify the criminal as the target of the warrant, and require all communications to or from the family's internet service to be intercepted. Attribute based interception would allow the agency to apply for a warrant to intercept the criminal's communications, but would allow the agency and issuing authority to use more targeted attributes to describe the communications that the service provider should access and deliver to the agency, such as the webmail account, the time of day, and the email addresses belonging to the criminal associates.

Attribute-based interception would allow for more targeted access to communications by ensuring that all the probative evidence is collected while minimising the lawful collection of irrelevant communications.

The Department's preliminary view is that, under this approach, a warrant would describe the communications to be lawfully accessed by way of a combination of attributes that identify the person of interest's communications.

The United Kingdom adopted an attribute-based interception model in 2000, under the *Regulation of Investigatory Powers Act 2000* (UK). The Act relevantly provides that a warrant must state the 'addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.'[35]

Warrant variation

The practice of sophisticated criminals and terrorists to swap between and discard multiple telecommunications services and devices—colloquially referred to as 'burner phones'—in an attempt to defeat lawful investigation is a long-standing problem. The *Telecommunications (Interception) Legislation Amendment Act 2000* introduced 'named person warrants' as a direct response to this tactic. These warrants authorise access to any telecommunications service that the person named on the warrant uses or is likely to use during the currency of the warrant. This provides agencies with the operational flexibility necessary to compensate for suspects' using multiple services in order to defeat investigation.

Attribute-based interception, as outlined above, would enable agencies and issuing authorities to adopt a more targeted approach to lawful access. In the above example, an agency limits the operation of the warrant to a particular email account and a timeframe linked to the *modus operandi* of the criminal. The corollary of this, however, is that warrants may tend to be narrower in scope, providing opportunities for sophisticated criminals to evade investigation by altering their communications habits in a similar way as 'burner phones'. That is, the target may begin to use different email accounts at different times to ensure that their communications with their criminal associates are not identified.

Consistent with PJCIS Recommendation 7, the Department's preliminary view is that a reformed TIA Act should provide that, subject to parameters set by issuing authorities, law enforcement, anti-corruption and national security agencies may vary the attributes describing the

[35] *Regulation of Investigatory Powers Act 2000* (UK), s 8.

communications to be lawfully accessed . This would allow agencies to remain responsive to changes in a person of interest's communication habits over the duration of a warrant. That is, if the person begins using a new email account to organise their criminal activities, the agency could vary the warrant accordingly.

Additionally, as an agency develops a better understanding of a person of interest's communications over the course of an investigation, the agency may be able to vary a warrant to 'filter out' communications that are not pertinent. This would enable an agency to exclude communications that are not relevant, reducing the volume of information lawfully accessed under the warrant.

Warrant variation would be a significant power and, as such, would also need to be subject to significant safeguards. The Department's preliminary view is that these safeguards might include:

- the ability for the issuing authority to set parameters around the variation of the warrant, for instance, prohibiting an agency from adding or removing given attributes
- a requirement that the officer authorising the variation be satisfied of the same criteria as the issuing authority in respect of the warrant-as-issued
- a requirement that agencies either revoke or narrow the scope of a warrant if the criteria on which it was issued are no longer satisfied, and
- oversight by the IGIS, in the case of ASIO, or the relevant oversight body, such as the Commonwealth Ombudsman, in the case of law enforcement and anti-corruption agencies.

Ensuring that agencies are able to lawfully access communications in an intelligible form

The power to lawfully access communications is only of value if agencies are able to interpret and act upon lawfully accessed information. As the Blunn Report concluded:[36]

> *The ever increasing range of data products carried over networks, often as a service to other providers, means that that data is often not readily interpreted by the carrier. From the point of view of the intercepting agencies receiving the raw data is of little use and defeats the intention of the scheme which pre-supposes product in useable form.*

Agencies historically relied on the small number of service providers in the Australian marketplace to deliver lawfully accessed communications in an intelligible form. The increasing diversity of the telecommunications industry, including the emergence of ancillary service providers, is limiting the effectiveness of such arrangements. Agencies are required to engage with an ever-wider range of providers to maintain their capabilities, many of whom may have had little or no previous engagement with the law enforcement or national security communities.

The Department is also advised that sophisticated criminals and terrorists are exploiting encryption and related counter-interception techniques to frustrate law enforcement and security investigations, either by taking advantage of default-encrypted communications services or by adopting advanced encryption solutions.

The Department's current view is that law enforcement, anti-corruption and national security agencies should be permitted to apply to an independent issuing authority for a warrant authorising the agency to issue 'intelligibility assistance notices' to service providers or other persons. The

---

[36] A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) 47.

issuing authority should be permitted to impose conditions or restrictions on the scope of this authority.

Where issued to a service provider, such notices would formalise existing arrangements. Providers would be eligible for compensation on a no profit, no loss basis and would not be subject to criminal liability for failing to comply with such notices—the industry enforcement regime established by the TIA Act and Telecommunications Act would apply.

When issued to a person other than a service provider, such as the subject of a warrant, the Department's preliminary view is that a notice would operate in a similar fashion to orders made under section 3LA of the *Crimes Act 1914*. Section 3LA permits agencies that have seized physical hardware, such as a computer or an external hard drive, under a search warrant to apply for a further warrant requiring a person to 'provide any information or assistance that is reasonable and necessary' to allow information held on the device to be converted into an intelligible form.

Under this approach, the person receiving a notice would be required to provide 'information or assistance' to place information obtained under the warrant into an intelligible form. The person would not be required to hand over copies of the communication in an intelligible form, and, a notice would not compel a person to do something which they are not reasonably capable of doing. Failure to comply with a notice would constitute a criminal offence, consistent with the Crimes Act.

The above approach is consistent with the approach taken by the United Kingdom, which permits officials of law enforcement and national security agencies to, where authorised under a warrant, issue a notice requiring a person to provide assistance in connection with accessing encrypted communications.[37] Similarly, South African law permits agencies to apply to a judicial officer for a direction requiring a person to provide information to the agency to enable the agency to decrypt lawfully intercepted communications.[38]

Reforming lawful access to telecommunications data

At present, a limited number of officers in enforcement, anti-corruption and national security agencies may authorise a carrier or carriage service provider to disclose telecommunications data. Many agencies use these provisions, including local government authorities and non-government organisations that have statutory responsibilities for the enforcement of certain laws, such as laws against animal cruelty.

The ability to obtain telecommunications data is a key investigative tool for Australia's law enforcement, anti-corruption and national security agencies. Data is used in almost every significant law enforcement and national security investigation, and its relative importance is growing as the use of encryption increasingly limits access to the content of communications.

Agencies require the ability to identify communications because criminals and terrorists use phones, email and the Internet to plan, organise and carry out criminal activities. The power to access telecommunications data is the tool that allows agencies to identify such communications.

The Department's view is that the increased complexity and sophistication of communications technologies justify the exploration of options for creating a more nuanced regime. A revised regime could, in particular, restrict access to telecommunications data to a narrower range of law enforcement, anti-corruption and national security agencies that have a demonstrated investigative need for access to that range of information, and which are subject to independent oversight.

---

[37] *Regulation of Investigatory Powers Act 2000* (UK), ss 49 and 50.
[38] *Regulation of Interception of Communications and Provision of Communications-Related Information Act 2002* (South Africa), s 21.

Limiting the range of agencies that can access telecommunications data

Under the current regime, any enforcement agency may lawfully access telecommunications data in an investigation. The term 'telecommunications data' has come to encompass a broad range of different types of information. Whether or not a particular type of information is relevant to a given agency will depend on the type of agency seeking the data and the matter being investigated.

On 7 November 2012, the Department provided the PJCIS with the Department's working definition of telecommunications data, which is at **Attachment D**. A previous copy of this definition was provided to the Senate Legal and Constitutional Affairs Legislation Committee on 16 October 2012. This working definition distinguishes between two categories of data:

- information that allows the communication to occur, such as information about duration, location, billing and the communicating parties—referred to as 'traffic data', and
- information about the parties to the communications, such as an account-holder's name, address, billing information and telephone number—referred to as 'account-holder data'.

Attachment C explores these types of information in more detail.

The Department's preliminary view is that some enforcement agencies may not always require the type of information that can be derived from lawful access to traffic data. Limiting the range of agencies permitted to access traffic data would create a more nuanced regime.

This approach would allow the Act to adopt a more granular approach to oversight and public reporting requirements for agencies accessing traffic data. These issues are discussed further, below.

Consistent with PJCIS Recommendation 5, the Department recommends exploring options to:

- create certainty about which agencies are permitted to access account-holder data or traffic data
- ensure that agencies accessing any type of telecommunications data have a demonstrated need to do so, and
- ensure that all agencies with data-access powers are subject to appropriate oversight, as discussed below.

The PJCIS also recommended 'using the gravity of conduct…as the threshold on which access is allowed'. However, the Department's view is that this approach would not be consistent with Australia's international legal obligations. Under the Council of Europe's *Convention on Cybercrime*, Australia is required to make access to telecommunications data available for the investigation of all criminal offences.[39] Introducing a minimum threshold for access to telecommunications data would be inconsistent with this obligation. The imposition of safeguards, including restricting the range of agencies permitted to access such data would, however, be consistent with the Convention.[40]

---

[39] *Convention on Cybercrime*, opened for signature 23 November 2001, ETS 185 (entered into force 1 July 2004), art 14(2); see also Council of Europe, *Explanatory Report to the Convention on Cybercrime*, paragraph 141.

[40] *Convention on Cybercrime,* ibid, art 15.

Proposals to require agencies to obtain warrants to access telecommunications data

The Department is aware of proposals in Australia and overseas to require a warrant for obtaining telecommunications data. The Department considers that a more holistic approach, including limiting the range of agencies permitted to access traffic data and requiring such access to be subject to independent oversight, as outlined above, would enable Parliament to strengthen the existing regime without degrading agencies' capabilities or imposing a disproportionate burden on agencies and issuing authorities.

Restricting lawful access to telecommunications data would likely degrade the investigative capabilities of Australia's law enforcement, anti-corruption and national security agencies. As discussed under Part 1, above, agencies often require telecommunications data to 'fill the gaps' in their knowledge at the early stages of investigations, and to provide vital, historical information about persons of interest.

Telecommunications data is not the only tool available to agencies for these purposes. It does, however, have a set of irreplaceable characteristics that often make it the most appropriate tool for agencies:

- it is low risk—unlike the use of undercover officers, informants or physical surveillance, agencies can obtain valuable information without placing their officers, agents or operations at risk

- it is less resource intensive—many other investigative techniques would require agencies to deploy teams of specialist officers to obtain basic information about a target and their associates; lawful access to telecommunications data allows agencies to prioritise the use of these scare resources for the most critical investigations, and

- it is less privacy intrusive—telecommunications data allows agencies to obtain factual information about communications, such as with whom, when and where a person was communicating, which is useful at the early stages of an investigation. However, as telecommunications data does not include the content of a communication it does not disclose more sensitive information about a person's motivations or intentions, such as what a person was talking about or why they were communicating.

Cybercrime investigations—such as, online fraud, identity theft and child exploitation investigations—rely heavily on telecommunications data. Cybercrime includes:

- crimes where computers or other communications technologies are integral to the offence, such as online fraud, identity theft and the distribution of child exploitation material, and

- crimes targeting computers, such as hacking or unauthorised access to data.

The overall cost of cyber and major technology-enabled crime to Australia in 2012-13 has been estimated at $1.18 billion (US$1.06bn).[41]

In a cybercrime or cyber-attack, the communications passing between computers are the crime or attack. As such, access to telecommunications data is vital for law enforcement and national security agencies to detect, identify, investigate and prosecute such activities. In particular, access to telecommunications data is essential to connect online criminal activity to the real-world offender. As such, requiring agencies to obtain a warrant to access telecommunications data would amount to a *de facto* requirement for judicial authorisation to investigate cybercrime or cyber-espionage—crimes that Parliament has already endorsed agencies to investigate.

---

[41] Norton, *Norton Cybercrime Report 2013* (2013).

Providers typically store IP-based telecommunications data only for a very limited period of time, if at all. The delay necessarily associated with preparing a warrant application for telecommunications data, or even making an emergency application, would give rise to a real risk that critical IP-based telecommunications data would have been purged from a provider's systems by the time a warrant was issued and executed, frustrating cybercrime investigations.

Cybercrime is an inherently borderless crime. High-speed telecommunications networks span the globe, revolutionising global communications but also allowing criminals to perpetrate cybercrimes across borders with ease. The ability and willingness of law enforcement agencies to effectively share telecommunications data, such as the IP address behind a cyber-attack, with their counterparts in other jurisdictions in a timely fashion is, therefore, fundamental to most cybercrime investigations.

Additionally, telecommunications data is a vital 'building block' for other powers under the TIA Act—it provides vital evidence for agencies to be able to satisfy the legal test to obtain a warrant in most situations. For example, the TIA Act requires agencies to provide evidence that a person is using a particular telecommunications service,[42] and that information likely to be obtained under the warrant would be likely to assist with the relevant investigation.[43]

Lawfully accessed telecommunications data is generally vital evidence to meet these tests—account-holder data is used by agencies to prove that a particular service belongs to a particular person, and call-charge records are important evidence to show that the service is being used to communicate with other persons of interest.

Restricting lawful access to telecommunications data would limit the ability of law enforcement and national security agencies to employ what is often the lowest risk, least resource-intensive and least intrusive investigative tool. Cybercrime investigations would be seriously impacted, if not prevented entirely, by restricting timely access to such information. A warrant regime for telecommunications data would also potentially limit agencies' ability to use other telecommunications interception powers that rely on access to data to advance investigations.

Warrant applications are resource intensive, both for the applicant agencies and for the issuing authorities hearing the applications. The Department is of the view that introducing a warrant regime for telecommunications data would impose a significant burden on agencies and issuing authorities that is disproportionate to any benefits that might be achieved.

In the 2012-13 financial year, enforcement agencies made 319,874 authorisations for access to existing telecommunications data for the purpose of enforcing the criminal law.[44] Requiring agencies to meet stricter thresholds and tests, combined with resource limitations, would likely result in only a proportion of these authorisations being re-made as warrant applications. Each authorisation, however, was justified on a case-by-case basis as being 'reasonably necessary'. A warrant regime would not remove the operational imperative for access telecommunications data. As such, the Department considers that agencies would find it reasonably necessary to re-make a significant proportion of their authorisations as warrant applications, resulting in a substantial and sustained increase in the number of warrant applications.

For example, in the 2012-13 financial year, the ACC made 3,789 authorisations to access telecommunications data. During that same period the ACC made 195 applications for telecommunications interception warrants and 10 applications for stored communications warrants. Given that the ACC's primary responsibility is combating serious and organised crime, the

[42] TIA Act, s 46(1)(c).
[43] TIA Act, s 46(1)(d).
[44] Above n 8, 49.

Department considers that it is likely that a substantial proportion of the ACC's authorisations would be re-made as warrant applications, subject only to internal resource limitations.

Constrained resources within law enforcement and national security agencies and for issuing authorities would therefore likely result in the warrant application process becoming an investigative 'bottleneck', limiting the ability of agencies to effectively investigate serious crime and national security matters.

Additionally, given the way in which telecommunications data is used in investigations, the time necessarily involved in preparing, reviewing and granting a warrant application to access such data would:

- significantly delay and, in some circumstances, undermine law enforcement and national security investigations
- impede operational activity, including the prevention of criminal acts, and
- divert scarce investigative resources during the critical, initial stages of an investigation.

In particular, the Department would be concerned that, even if accompanied by increased resourcing, such a warrant regime would distort the ability of issuing authorities to perform their day-to-day functions as members of the judiciary or AAT.

Similar views have been expressed internationally. The UK Interception of Communications Commissioner, an independent statutory officer responsible for the oversight of lawful access to telecommunications data, has stated that requiring judicial authorisation of access to telecommunications data would not 'have any impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data.'[45]

In February 2013, the UK Intelligence and Security Committee reached a similar conclusion:[46]

> *Any move to introduce judicial oversight of the authorisation process could have a significant impact on the Agencies' operational work… We are not convinced that such a move is justified in relation to the Agencies, and believe that retrospective review by the Interception of Communications Commissioner, who provides quasi-judicial oversight, is a sufficient safeguard.*

In the US, the President's Review Group on Intelligence and Communications Technologies recommended that judicial authorisation be required for the Federal Bureau of Investigation to issue 'National Security Letters', which authorise lawful access to telecommunications data.[47] The Director of the Administrative Office of the United States Courts has expressed concern at this recommendation, stating that:[48]

> *[E]ven if one assumes that adequate resources can be made available to the [Court]… jurisdiction over 21,000 NSL requests per year would transform the [Court] from an institution that is primarily focused on a relatively small number of cases that involve the most intrusive or expansive forms of intelligence collection to one primarily engaged in processing a much larger number of more routine, subpoena-type cases. We fear that such a drastic shift of emphasis would diminish the [Court's] effectiveness in adjudicating and overseeing cases involving electronic surveillance*

---

[45] Sir Paul Kennedy, *2012 Annual Report of the Interception of Communications Commissioner*, 63.
[46] Intelligence and Security Committee, United Kingdom Parliament, *Access to communications data by the intelligence and security Agencies* (2013) 26.
[47] President's Review Group in Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (2013) 24.
[48] Enclosure to letter from Judge John D. Bates to Senator Dianne Feinstein, *Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act*, 13 January 2014, 9.

For further information, please see the Department's submission to the Senate Legal and Constitutional Affairs Legislation Committee's inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013, which is at **Attachment F**.

Simplifying provisions for dealing with and collaborating on the use of sensitive material

Lawfully accessed information and information about investigations must be guarded to protect the privacy of Australians and the security of such investigations. To this end, the TIA Act heavily restricts the circumstances in which law enforcement, anti-corruption and national security agencies may use or disclose lawfully accessed information, and imposes detailed requirements about record-keeping, retention and destruction of such information.

At the same time, agencies must have sufficient operational flexibility to deal with and share protected information to allow them to fulfil their legislated functions, including collaborating with other agencies. In its submission to the PJCIS, the AFP explained that:[49]

> *The complex and evolving nature of transnational crime mean that no one agency can effectively conduct complex investigations. Collaboration is an essential element in achieving operational goals.*

The Department's view is that the current provisions are overly complex and, in some cases, may represent a barrier to effective information sharing and collaboration both within an agency and between Australia's law enforcement, anti-corruption and national security agencies. In evidence to the PJCIS, Commissioner Scipione of the New South Wales Police Service provided examples of the challenges faced by agencies:[50]

> *[I]f we were tapping a telephone and, as a result of some information which came across that phone, we had concerns that someone was carrying a firearm on the street but we were not in a position to take any action, we cannot post that intelligence on a warning system for our officers. We would like to be able to put out a warning saying, 'If you pull this vehicle over with that person driving, be careful—intelligence suggests that they are armed.'*
>
> *Another example might be where we have an interception operation running and, as a result of that, we come across some information about a child abuse situation. In that setting, we are not at liberty even to advise a child protection authority that there is a telephone interception running. That is because we are not able to use that lawfully intercepted information. That is difficult. We encounter that every day.*

Law enforcement, anti-corruption and national security agencies have well-established processes for controlling and handling highly classified and sensitive information. The additional, prescriptive layer of controls under the TIA Act, which was developed in 1979, does not address the complexity of the contemporary investigative environment. The Department's preliminary view is that a revised TIA Act should adopt a more flexible and principles-based system for using and disclosing interception-related material. Under this approach, agencies would be permitted to use or share information:

- in connection with the purpose for which the information was lawfully obtained
- for the investigation of serious crime, corruption and threats to national security
- for the purpose of administrating the interception regime

---

[49] Australian Federal Police, Submission no 163 to the Parliamentary Joint Committee on Intelligence and Security, *Inquiry into Potential Reforms to Australia's National Security Legislation*, 20 August 2012, 10.

[50] Above n 32, 25.

- in emergency situations, and
- for a limited number of secondary purposes, including the investigation of offences that meet a minimum threshold or serious misconduct of an official, mutual assistance and extradition matters, ACC investigations and operations, and the functions of ASIO or anti-corruption agencies.

This approach would not substantially change the policy intent for which agencies may deal in interception-related information. Instead, the Department's current proposal is to develop a more transparent and efficient regime that is easier for officials and the public to understand and apply, which allows agencies to rely on established information handling protocols, and which requires fewer amendments over time.

Strengthening the oversight and accountability framework

The power to access communications is an important but intrusive investigative tool for Australia's law enforcement and national security agencies. As such, the TIA Act strictly limits the circumstances in which agencies may lawfully access communications and how agencies may deal with accessed information. The Act then sets out various oversight and accountability measures to ensure that agencies respect these limits and act with propriety.

The current oversight and accountability framework

Robust and transparent oversight arrangements are important for maintaining the confidence and trust of the Australian Government, national and international partners and the Australian community. The current oversight and accountability arrangements under the regulatory regime include:

- requiring agencies to maintain records of their use of powers under the Act, and of their use of information obtained under the Act
- establishing a detailed inspection and reporting regime for law enforcement agencies in relation to live interception and access to stored communications
- oversight of ASIO under the IGIS Act, and
- dedicated criminal and civil penalty regimes for breaches of the TIA Act.

The power to access communications, while vital to investigations, is only one of the investigative tools available to Australia's law enforcement, anti-corruption and national security agencies. As such, in addition to the requirements set out in the TIA Act, interception falls under the general oversight and accountability measures that apply to these agencies, including:

- statutory codes of practice, such as the professional standards orders issued by the Commissioner of the AFP under s 40RC of the *Australian Federal Police Act 1979*
- ministerial guidelines, such as the guidelines issued to ASIO by the Attorney-General under s 8A of the *Australian Security Intelligence Organisation Act 1979*, which are to be observed in the performance by the Organisation of its functions or the exercise of its powers
- internal professional standards and compliance teams, which are responsible for developing and maintaining professional standards throughout organisations including the oversight and investigation of complaints about the conduct of officials
- security clearances—typically to the highest levels in the case of staff involved in telecommunications interception—which involve ongoing inquiries into and corroboration of a

person's background, character and personal values to ensure that an individual is suitable to be granted access to sensitive and classified information

- external oversight by organisations such as the Commonwealth Ombudsman and the IGIS, both of which have powers akin to those of a standing Royal Commission
- external oversight by anti-corruption agencies, such as the Australian Commission for Law Enforcement Integrity
- the ability for the officials of law enforcement and national security agencies to report and disclose information about suspected or probable illegal conduct or other wrongdoing to oversight agencies and, in certain cases, the public, such as under the *Public Interest Disclosures Act 2013*, and
- judicial scrutiny of agencies' conduct in court.

The importance of these oversight and accountability arrangements goes beyond the headline results they achieve. These arrangements have a normative effect within agencies, promoting cultures of integrity, compliance and continuous improvement.

The Australian Intelligence Community, of which ASIO is a member, has been described by key academics as 'one of the most accountable in the Western world in terms of oversight and responsiveness to audit and inquiry'.[51] The IGIS model has been used as an example for foreign governments seeking to strengthen their own oversight regimes.[52]

Reforming the oversight and accountability framework

Nevertheless, the Department's current view is that there are several areas where the existing oversight arrangements could potentially be strengthened or improved as part of the reform of the TIA Act, consistent with PJCIS Recommendation 4. These include:

- extending the inspection and reporting regime to apply to law enforcement and anti-corruption agencies' access to and dealing in traffic data
- restructuring the oversight arrangements so that a single oversight agency has the ability to comprehensively oversight law enforcement and anti-corruption investigations, including agencies' interception activities, access to traffic data, use of other exceptional powers, and broader functions and activities, and
- granting Commonwealth, State and Territory oversight agencies greater flexibility to determine how best to oversight the law enforcement and anti-corruption agencies within their purview—and in particular to establish consistent oversight practices across the full breadth of an agency's functions and activities—subject to strict minimum standards established by the reformed Act.

Progressing these policy proposals would require close engagement with investigative and oversight agencies, to ensure that the oversight regime under a revised TIA Act is effective, efficient and sufficiently flexible to apply to each agency. Close engagement with State and Territory governments would also be required to ensure jurisdictional considerations are addressed.

---

[51] J. Blaxland and R. Crawley, 'Intelligence oversight and accountability: who watches the watchers?', *The Conversation* (online), 11 December 2013, < http://theconversation.com/intelligence-oversight-and-accountability-who-watches-the-watchers-21112>

[52] IGIS, *Annual Report 2012-13* (2013) 5.

Improving the effectiveness and efficiency of the public reporting requirements

The TIA Act's annual reporting regime provides useful information to the public and Parliament about the operation of the regime with respect to law enforcement agencies. The information tracks the usage of different powers over time to provide transparency about the operation of the regime.

The Department's preliminary view is that the current reporting requirements could be revised to improve their effectiveness and efficiency by:

- providing greater guidance to law enforcement and anti-corruption agencies on how to report the required information, to reduce the risk of inconsistencies between information reported by different agencies
- separately reporting the figures for lawful access to traffic and subscriber data by law enforcement and anti-corruption agencies, to ensure that members of the public have a clear picture about the level of lawful access to each category of telecommunications data, and
- providing more detailed information about the role of issuing authorities in scrutinising warrant applications under the Act, to increase public understanding of the importance of the role of issuing authorities in oversighting lawful access to communications.

For example, the TIA Act requires reporting about the number of times an application for a warrant was refused by an issuing authority. However, no data is collected about the number of times an issuing authority has required the agency to obtain and provide additional information before issuing a warrant. The result is that data about refusals does not fully reflect the level of scrutiny applied by issuing authorities to warrant applications and so may lead readers of the Annual Report to draw inaccurate conclusions.

The Department has made efforts to provide greater transparency and insight into the use of interception powers in the 2012-13 Annual Report, by increasing the amount of contextual information contained in the report, as well as by drafting the report in a more accessible format. In the Department's view, further progress would require legislative change.

Consistent with PJCIS Recommendation 3, the Department recommends exploring options to increase the effectiveness of the reporting regime by ensuring that important and relevant data is collected and made available to the public, and to ensure that the quality of the data collected is sufficient to support robust analysis. Revising the reporting requirements also has the potential to drive administrative efficiencies within agencies, and within the Department, by ensuring that only probative data is collected.

Regulation of the telecommunications industry

Telecommunications industry participants provide essential assistance to the law enforcement and national security agencies under the TIA Act. However, the telecommunications industry has changed dramatically since 1979. Telecom Australia is no longer the monopoly provider of telecommunications in Australia. In June 2013, there were 201 licenced carriers[53] providing a wide range of services such as the mobile phone networks managed by Telstra, SingTel Optus and Vodafone Hutchison Australia to free, city-wide Wi-Fi networks, and machine-to-machine networks used for tracking commercial assets and infrastructure.

Additionally, the development of IP-based communications and networks is leading to the diversification of the telecommunications industry. Any person can now write an application or build a service—referred to in the submission as 'ancillary service providers'—that allows

[53] Above n 3, 13.

communications 'over the top' of carrier networks and carriage services, such as Skype, Facebook, Gmail, Whatsapp or Snapchat. There are now millions of applications available for download onto smartphones, tablets and other communications devices, many of which enable communications. All of these changes mean that it is increasingly difficult to draw the line between 'telecommunications' and 'technology' companies.

A core focus of the revision of the TIA Act should be on ensuring that the obligations imposed on the telecommunications industry are both effective and sustainable in the modern telecommunications environment.

The current industry assistance regime

Telecommunications industry participants play an invaluable role in assisting Australia's law enforcement, anti-corruption and national security agencies to lawfully access communications under the TIA Act.

The TIA Act requires all carriers and carriage service providers to develop and maintain a general interception capability.[54] This means the ability to intercept communications that are being carried by a service provided by the carrier or carriage service provider and to deliver those communications to a requesting agency in accordance with a warrant.

Additionally, under the Telecommunications Act, carriers and carriage service providers have an obligation to provide such help to agencies as is 'reasonably necessary' for enforcing the criminal law and laws imposing pecuniary penalties, protecting the public revenue and safeguarding national security. This can include providing assistance to agencies in executing a warrant issued under the TIA Act.[55]

Under the Telecommunications Act, the cost of developing and maintaining interception capability is borne by carriers and carriage service providers, while the cost of capabilities to deliver lawfully accessed information to an agency is borne by interception agencies.[56] The costs have been split on that basis because industry is best placed to find efficiencies and to minimise costs in relation to their own systems and services.

Reforming the industry assistance framework

The industry assistance obligations set out in Chapter 5 of the TIA Act are predicated on the existence of one or few service providers, each providing similar services and possessing similar resources and customer bases. However, the modern telecommunications environment no longer reflects this assumption.

The Department's preliminary assessment is that the comprehensive revision of the TIA Act may provide a range of opportunities to modernise the industry assistance framework, including:

- ensuring that the scope of the framework is fit-for-purpose and appropriate for the modern telecommunications environment—in particular, by ensuring that the framework applies to ancillary service providers, consistent with PJCIS Recommendation 14
- exploring models for interception capability obligations that reduce the existing regulatory burden on carriers and carriage service providers, and mitigate the regulatory burden for newly-regulated ancillary service providers, consistent with PJCIS Recommendation 11

---

[54] TIA Act, s 191.
[55] Evidence to the Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, Canberra, 30 May 2013, 43 (Michael Phelan, Deputy Commissioner, AFP).
[56] TIA Act, Part 5-6.

- strengthening information security obligations for service providers holding information relating to the lawful access regime, reflecting the highly sensitive nature of this information
- exploring options to ensure that the enforcement processes and powers are structured to encourage negotiated and mutually-agreed outcomes with a revised industry assistance framework, consistent with PJCIS Recommendation 12, and
- removing low value-add and burdensome obligations from industry participants, such as the requirement to provide annual Interception Capability Plans (ICPs).

Mandatory telecommunications data retention

Telecommunications data retention refers to the storage of traffic and subscriber data. Service providers routinely engage in telecommunications data retention for their business purposes. A mandatory telecommunications data regime, by comparison, would involve requiring service providers to retain a defined set of traffic and subscriber data for a set period, for example, two years.

Mandatory data retention would not involve mass surveillance or the collection and analysis of telecommunications data in bulk. It is important to distinguish between a requirement that service providers keep certain records for a specified period of time—mandatory data retention—and the circumstances in which agencies may lawfully access and analyse that information, which are governed by the data authorisation provisions of the TIA Act. No proposal would alter the basis for lawful access to telecommunications data. Agencies would continue to be permitted to make authorisations for access to specific telecommunications data in limited circumstances and subject to appropriate safeguards.

The Department notes that mandatory data retention requirements are not a novel concept at Australian law. A range of other Australian industries are subject to data retention requirements that apply to personal information for law enforcement and national security purposes, including the banking and financial services industries under the *Proceeds of Crime Act 1987* and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, and certain participants in the air and sea freight industries under the *Customs Act 1901*.

Historically, service providers have generated and retained telecommunications data for their business purposes. However, as providers shift to modern, IP-based networks and services, they are tending to retain a narrower range of data, and to retain that data for shorter periods. This trend is already degrading the investigative capabilities of law enforcement, anti-corruption and national security agencies, and is expected to continue.

The PJCIS identified this trend in industry business practices and concluded that it is resulting in the actual and accelerating degradation of the investigative capabilities of Australian agencies.[57] This conclusion is consistent with the findings of a number of international jurisdictions and bodies, including the UK Intelligence Services Committee (UK ISC)[58] and the European Commission.[59]

Mandatory data retention, if implemented, would be a direct response to these changing business practices and the impact they are having on the investigative capabilities of law enforcement, anti-corruption and national security agencies, not just in Australia, but across the world.

---

[57] Above n 2, paragraph 5.207.

[58] Intelligence and Security Committee, United Kingdom Parliament, *Access to communications data by the intelligence and security Agencies* (2013) paragraphs 29 and 39.

[59] European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, COM/2011/0225 FIN (2011), 4.

The PJCIS recommended (PJCIS Recommendations 42 and 43) that any decision about whether to implement a data retention regime 'is ultimately a decision for Government', and that if the Government were persuaded that such a regime should proceed, Government should publish exposure draft legislation and refer it to the PJCIS for examination. The Committee also recommended that any such draft legislation should contain an array of control measures aimed at protecting individual privacy and the integrity of the regime as a whole.

The Department generally supports the principles contained in these recommendations. However, the Department has not had the opportunity to consult with interested stakeholders, including the telecommunications industry or privacy advocates.

The Department agrees with the PJCIS's assessments that a mandatory telecommunications data retention regime would be of significant utility for intelligence, counter-terrorism and law enforcement investigations,[60] that such a regime would raise fundamental privacy issues,[61] and that those issues should be sufficiently addressed before any such regime is progressed.[62]

The Department considers that further exploration of options is necessary and that detailed consultation needs to occur with key stakeholders, including the telecommunications industry and privacy advocates before providing detailed advice to Government to support any decision on this topic.

[60] Above n 2, 5.207.
[61] Ibid, paragraph 5.208.
[62] Ibid.

Attachment A: AGD views on PJCIS recommendations relating to telecommunications interception

The Department provides its preliminary views on the PJCIS's recommendations below, but notes that these preliminary views will require further development following consultation with stakeholders, including interception agencies, oversight bodies, warrant issuing authorities, State and Territory governments and privacy advocates. The Department's preliminary views do not necessarily reflect the views of Government.

Recommendation	AGD preliminary view

Recommendation 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
  o to protect the privacy of communications
  o 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*.
	The Department's preliminary view is to support this recommendation in principle.

Recommendation	AGD preliminary view
Recommendation 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.	The Department's preliminary view is to support recommendation 2 in principle.
Recommendation 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.	The Department's preliminary view is to support recommendation 3.

Recommendation	AGD preliminary view
Recommendation 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.	The Department's preliminary view is to support recommendation 4.
Recommendation 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.	The Department's preliminary view is to support recommendation 5 in principle. The Department notes that the Council of Europe *Convention on Cybercrime*, to which Australia is a party, prohibits increasing the access threshold for data itself.
Recommendation 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.	The Department's preliminary view is to support recommendation 6.

Recommendation	AGD preliminary view
Recommendation 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.	The Department's preliminary view is to support recommendation 7 in principle.

Recommendation	AGD preliminary view
Recommendation 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.	The Department's preliminary view is to support recommendation 8 principle.
Recommendation 9 The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* be amended to remove legislative duplication.	The Department's preliminary view is to support recommendation 9.

Recommendation	AGD preliminary view
Recommendation 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.	The Department's preliminary view is to support recommendation 10.

Recommendation	AGD preliminary view
Recommendation 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*.	The Department's preliminary view is to support recommendation 11.
Recommendation 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.	The Department's preliminary view is to support recommendation 12 in principle.
Recommendation 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.	The Department's preliminary view is to support recommendation 13 in principle.
Recommendation 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.	The Department's preliminary view is to support recommendation 14 in principle.

Recommendation	AGD preliminary view
Recommendation 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.	The Department's preliminary view is to support recommendation 15 in principle.
Recommendation 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.	The Department's preliminary view is to support recommendation 16 in principle.
Recommendation 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.	The Department's preliminary view is to support recommendation 17.

Recommendation	AGD preliminary view
Recommendation 18 The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* 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.	The Department supports recommendation 18.

Recommendation	AGD preliminary view
Recommendation 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 meta-data 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.	The Department's preliminary view is to support the principles contained recommendation 42. However, the Department has not had the opportunity to consult with interested stakeholders, including the telecommunications industry or privacy advocates. The Department considers that further exploration of options is necessary and that detailed consultation needs to occur before providing detailed advice to Government to support any decision on this topic.

Recommendation	AGD preliminary view
Recommendation 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.	The Department's preliminary view is to support the principles contained in recommendation 43. In particular, the Department would support including rigorous oversight and review mechanisms as a part of any mandatory data retention regime. However, the Department has not had the opportunity to consult with interested stakeholders, including the telecommunications industry or privacy advocates. The Department considers that further exploration of options is necessary and that detailed consultation needs to occur before providing detailed advice to Government to support any decision on this topic.

Attachment B: AGD views on ALRC recommendations

ALRC Recommendation	AGD view
Recommendation 71-2 The Australian Government should initiate a review to consider whether the Telecommunications Act and the Telecommunications (Interception and Access) Act continue to be effective in light of technological developments (including technological convergence), changes in the structure of communications industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider: a) whether the Acts continue to regulate effectively communications technologies and the individuals and organisations that supply communication technologies and communications services; b) how these two Acts interact with each other and with other legislation; c) extent to which the activities regulated under the Acts should be regulated under general communication 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.	Since the ALRC released its report in 2008, the PJCIS has made a number of specific recommendations in relation to the TIA Act, including that the Act be comprehensively revised. Additionally, this Committee has commenced a further inquiry into the comprehensive revision of the TIA Act.

Attachment C: Commonly-used terminology

The TIA Act is a complex statute, as are the fields of communications privacy and lawful access more generally. There are a range of uncommon or specialised terms. The Department has attempted to explain a number of important and frequently-encountered terms, below.

Access refers to obtaining information from a service provider. The term is used within the TIA Act to specifically refer to obtaining the content of a stored communication from a provider, but is also used more generally to refer to obtaining telecommunications data from a provider. If a single term is used to mean both 'interception' of live communications and 'access' to stored communications, the preferred term is 'access to communications'.

Content of a communication means the 'substance' of a communication, being what is spoken or typed, or the core of what is being communicated.

Interception refers to the capturing of the content of a communication in its passage across a network. That content is captured by a carrier or carriage service provider exercising a technical capability called '**interception capability**'.

Interception warrants authorise the interception of the content of communications in their passage across a network, as well as access to any associated telecommunications data.

Metadata is a term often used to mean telecommunications data. Metadata may have further meanings to technical users of the term. For example, metadata may refer to information produced by analysing other, aggregated data. To avoid confusion, this submission uses the term telecommunications data.

Privacy has two related meanings in the context of the TIA Act.

- **Privacy protections** are the rules that protect people from eavesdropping (without their knowledge or consent) by third parties. These protections facilitate confidence in telecommunications and allow people to have personal conversations, conduct banking or buy and sell goods online.

- **Proportionality requirements** refer to the rules that require agencies to follow due process and act appropriately with a mind to proportionality when lawfully exercising their powers are also a kind of privacy protection. These rules offer the community a range of explicit, legislative assurances requiring Government to do the right thing when exercising intrusive and exceptional powers. This second type of protection is better referred to as '**propriety**', '**proportionality requirements**' or '**safeguards**' to prevent confusion with the primary meaning of privacy.

Stored communication means a communication, such as an SMS message or email, while it is held by a carrier or carriage service provider. That is, a private communication that has ceased passing over a network and is being held by a provider. An email or SMS message held on a user's computer or phone is not a stored communication.

Stored communications warrants authorise access to stored communications held by a carrier or carriage service provider. Both interception and access refer to covert processes – meaning that the subject of the warrant is not made aware of its existence. Other Commonwealth, State and Territory laws include other forms of warrants, often called '**overt search warrants**'. The distinction between overt and covert powers is important when considering thresholds for using powers. Covert powers tend to require an agency to meet a higher threshold than analogous overt powers.

Telecommunications data refers to information or documents that are not the content of a communication. The Department's working definition of telecommunications data, which provides greater detail about the types of information that are telecommunications data, is at **Attachment D**.

At times, the distinction between 'telecommunications data' and 'content of a communication' may become less clear. This is particularly the case for information that, while not obviously the 'substance' of a communication, could contain or reveal substantive information, such as:

- email subject lines—subject lines can be used to convey the substance of a communication, and
- Uniform Resource Locators (URLs)—the details of which web page a person visited can reveal the content that a person accessed.

To avoid confusion and minimise the potential for undue intrusions on privacy, the Department's advice to agencies, industry participants and the public is that any information that contains or reveals the content of a communication is protected by the prohibitions on interception and access to content under sections 7 and 108 of the TIA Act.

Telecommunications data can be further divided into two elements:

- **Account-holder data** refers to information about the holder of a communications account, such as names, addresses, billing information and telephone numbers, and
- **Traffic data** refers to information with a closer nexus to a particular communication, such as information about duration, location, billing and the communicating parties.

Attachment D: Definition of telecommunications data

Definition of Telecommunications Data

Also known as Metadata, Communications Data and Communications Associated Data

Telecommunications data falls into 2 categories:

1. **Information that allows a communication to occur**
2. **Information about the parties to the communications**

Relates to communications for:

1. telephones – both fixed and mobile
2. Internet

Information that allows a communication to occur:

- The Internet identifier (information that uniquely identifies a person on the Internet)assigned to the user by the provider
- For Mobile service: the number called or texted.
- The service identifier used to send a communication, for example the customer's email address, phone number or VoIP number.
- The time and date of a communication.
- General location information, ie cell tower.
- The duration of the communication.

Information about the parties to the communications is information about the person who owns the service. This would include:

- Name of the customer
- Address of the customer
- Postal address of the customer (if different)
- Billing address of the customer (if different)
- Contact details, mobile number, email address and landline phone number
- Same information on recipient party if known by the service provider.

The definition of telecommunications data <u>does not</u> include information relating to a person's web browsing or the contents or substance of their communications.

Attachment E: Amendments to the TIA Act since 2000

Amending Act	Description
Telecommunications (Interception) Legislation Amendment Act 2000	Introduced named person interception warrants and other measures
Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000	Technical amendment. Related to money laundering offences being serious offences in TIA Act. The Amendment Act moved this offence from s83 Proceeds of Crime Act 1987 to s135.3 Criminal Code, and the TI Act was updated accordingly
Law and Justice Legislation Amendment (Application of Criminal Code) Act 2001	Applied to TI Act principles of criminal responsibility set out in Chapter 2 of Criminal Code. Clarified operation of the 'reasonable excuse' defence in relation to offences of obstruction (s106) or non-compliance with inspections (s107).
Corporations (Repeals, Consequentials and Transitionals) Act 2001	Technical amendment. Updated references to 'Corporations Law' in TI Act to 'Corporations Act 2001'.
National Crime Authority Legislation Amendment Act 2001	Technical amendment. Substituted references in TI Act to 'Chairman' of National Crime Authority (now ACC) with 'Chair'.
Royal Commissions and Other Legislation Amendment Act 2001	Enabled the Minister to declare that a Royal Commission can receive telecommunications interception information
International Criminal Court (Consequential Amendments) Act 2002	Included certain proceedings under the International Criminal Court Act within the definition of 'exempt proceedings' under the TI Act, allowing interception information to be given as evidence in those proceedings.
Telecommunications Interception Legislation Amendment Act 2002	Amongst other things, the Act allowed interception for terrorism and child pornography offences
Proceeds of Crime (Consequential Amendments and Transitional Provisions) Act 2002	Updated serious offence reference in s5D(4) TI Act to ensure interception may be authorised to occur in relation to the more serious money laundering offences in Part 10.2 Criminal Code.
Australian Crime Commission Establishment Act 2002	Technical amendment. Changed references to National Crime Authority to the new Australian Crime Commission.

Amending Act	Description
Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003	Amended TI Act so that people other than ASIO officers may communicate intelligence on behalf of ASIO, when authorised by the Director-General.
Telecommunications Interception and Other Legislation Amendment Act 2003	The amendment Act: • included the new WA Corruption and Crime Commission and WA Parliamentary Inspector of the Corruption and Crime Commission as eligible authorities able to receive interception information • allowed interception for offences relating to people smuggling, slavery, sexual servitude and deceptive recruiting
Telecommunications (Interception) Amendment Act 2004	The Act: • allowed interception for cybercrime offences • extended the protections of the Act in relation to text based communications • facilitated the recording of calls to publicly-listed ASIO numbers, • clarified the application of the Act to delayed access message services
Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004	Included child pornography, child abuse and child grooming offences committed over telecommunications systems as offences for which interception is available. Also technical amendments updating references to 'Part VIIB of the Crimes Act 1914' to 'Part 10.6 of the Criminal Code'.
Telecommunications (Interception) Amendment (Stored Communications) Act 2004	Excluded interception of stored communications from the prohibition against interception (these provisions are no longer in the Act)

Amending Act	Description
Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Act 2005	Amongst other things, the amendment Act: • allowed the interception without a warrant of communications to and from declared emergency services facilities • created an exception to the prohibition against interception to allow interception (without a warrant) by authorised radiocommunications inspectors fulfilling their statutory obligations under the *Radiocommunications Act 1992* • allowed interception for assisting a person to escape punishment for or dispose of the proceeds of certain serious offences
Criminal Code Amendment (Trafficking in Persons Offences) Act 2005	Updated references to people trafficking etc offences to reflect amendments made to these offences in Criminal Code.
Statute Law Revision Act 2005	Technical amendments. Removed obsolete references to organisations that no longer exist.
Intelligence Services Legislation Amendment Act 2005	Specified that if ASIO Director-General uses s10 emergency warrant, the Director-General must give a copy of the warrant to the IGIS within 3 working days.
Law and Justice Legislation Amendment (Serious Drug Offences and Other Measures) Act 2005	Made interception available in relation to offences against Part 9.1 of the Criminal Code (serious drug offences)
Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005	The Act temporarily extended the (now repealed) ability for interception agencies to obtain stored communications without a warrant. It also enabled more effective use of intercepted material by agencies involved in the investigation of corruption.
Telecommunications (Interception) Amendment Act 2006	Prohibited access to stored communications. Introduced a stored communications warrant regime.
Law Enforcement Integrity Commissioner(Consequential Amendments) Act 2006	Technical amendments relating to ACLEI.
Law and Justice Legislation Amendment (Marking of Plastic Explosives) Act 2007	Technical amendments relating to plastic explosive offences created by the amendment Act

Amending Act	Description
Telecommunications (Interception and Access) Amendment Act 2007	Amongst other things, the Act: • transferred provisions relating to access to telecommunications data from the Telecommunications Act to the TIA Act • provided a mechanism for access to prospective telecommunications data • imposed obligations on carriers and carriage service providers in relation to interception capability and delivery capability (transferring and clarifying provisions from the Telecommunications Act)
Telecommunications (Interception and Access) Amendment Act 2008	Amongst other things, the Act: • clarified agencies' reporting requirement under the TIA Act • clarified that multiple telecommunications devices can be intercepted on the one named person warrant
Telecommunications Interception Legislation Amendment Act 2008	Made amendments to address legal uncertainties about using legislative definitions to confer power to make an authorisation by including an express power to make authorisations
Telecommunications Interception Legislation Amendment Act (No. 1) 2009	Introduced Queensland Public Interest Monitor
Trade Practices Amendment (Cartel Conduct and Other Measures) Act 2009	Allowed interception for cartel offences in the new Competition and Consumer Act
Crimes Legislation Amendment (Serious and Organised Crime) Act 2010	Allowed interception for offences relating to membership etc of a criminal organisation. Also allowed sharing with police forces of interception information relating to criminal organisations.
Crimes Legislation Amendment (Serious and Organised Crime) Act (No. 2) 2010	Allowed interception for offences against Division 390 of the Criminal Code relating to criminal organisations. Allowed admission of interception evidence in proceedings for contempt of the Australian Crime Commission.
Statute Law Revision Act 2010	Technical amendments.
Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010	Ensured that interception warrants may be issued for the full suite of Commonwealth child sex offences, including new offences inserted into the Criminal Code by the amendment Act.

Amending Act	Description
Trade Practices Amendment (Australian Consumer Law) Act (No. 1) 2010	Technical amendment updating reference to schedule of Competition and Consumer Act
Anti-People Smuggling and Other Measures Act 2010	Updated references to people smuggling offences in the TIA Act and ensure that interception would be available for new offences of this kind creating by the Anti-People Smuggling and Other Measures Act 2010.
Freedom of Information Amendment (Reform) Act 2010	Technical amendment replacing reference to Privacy Commissioner with reference to Information Commissioner.
Trade Practices Amendment (Australian Consumer Law) Act (No. 2) 2010	Technical amendment replacing references to Trade Practices Act with references to Competition and Consumer Act
Corporations Amendment (No. 1) Act 2010	Allowed interception for market misconduct offences under the Corporations Act
Crimes Legislation Amendment Act 2011	Allowed sharing of interception information for purposes related to internal investigations of ACC staff for corruption.
Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011	Technical amendment to ensure that interception would continue to be available in relation to offence of conveying a thing into a jail to facilitate escape of a prisoner.
Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011	Amended the TIA Act, the ASIO Act and the Intelligence Services Act to enable greater cooperation, assistance and information sharing within Australia's law enforcement and national security communities
Acts Interpretation Amendment Act 2011	Technical amendment to update reference to Acts Interpretation Act
Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Act 2012	In relation to TIA Act, permitted the provision of interception material to a foreign country in extraditions and made other consequential amendments
Telecommunications Interception and Other Legislation Amendment (State Bodies) Act 2012	Added the Victorian IBAC, the Victorian Inspectorate and the South Australian Independent Commissioner Against Corruption as eligible authorities under the TIA Act able to receive interception information. Also introduced the Victorian Public Interest Monitor.

Amending Act	Description
Cybercrime Legislation Amendment Act 2012	Implemented Australia's obligations under the Cybercrime Convention. Changes to the TIA Act included: • allowing preservation of telecommunications data for investigations • ensuring Australian agencies are able to obtain and disclose telecommunications data and stored communications for foreign investigations
Law Enforcement Integrity Legislation Amendment Act 2012	Amended the TIA Act and other relevant legislation to introduce targeted integrity testing for members of the AFP, ACC and Customs suspected of corrupt conduct. Allowed an interception agency to provide intercepted information to Customs, AFP, ACC or ACLEI for integrity testing purposes.
Crimes Legislation Amendment (Slavery, Slavery-like Conditions and People Trafficking) Act 2013	Amended the Criminal Code Act to introduce new offences of forced labour, forced marriage, harbouring a victim, and organ trafficking. Also amended the TIA Act to make interception available in relation to these offences and slavery offences as redefined by the Amendment Act.
Federal Circuit Court of Australia (Consequential Amendments) Act 2013	Removed references to 'Federal Magistrate' no longer required after creation of Federal Circuit Court
Crimes Legislation Amendment (Law Enforcement Integrity, Vulnerable Witness Protection and Other Measures) Act 2013	Technical amendments updating references to the Victorian IBAC Act
Statute Law Revision Act 2013	Technical amendment.

Attachment F: Submission to the inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013

Attorney-General's Department Submission to the Senate Standing Committee on Legal and Constitutional Affairs Telecommunications Amendment (Get a Warrant) Bill 2013

1. SUMMARY

The Telecommunications Amendment (Get a Warrant) Bill 2013 (the Bill) seeks to amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to require law enforcement and national security agencies to obtain a 'stored and other communications' warrant to access telecommunications data held by a carrier or carriage service provider (a provider) for the purpose of investigating a criminal offence.

If enacted, the Bill would significantly affect the ability of law enforcement and national security agencies to perform their legislated roles, would contravene Australia's international obligations under the Council of Europe's *Convention on Cybercrime* (the Cybercrime Convention) to which Australia is a party, and would have the unintended consequence of eroding personal privacy protections.

In the Department's submission to the Parliamentary Joint Committee on Intelligence and Security's (the PJCIS) 2012 Inquiry into Potential Reforms of National Security Legislation, the Department noted that the magnitude of current and anticipated change to the telecommunications landscape means it is now timely to consider whether the privacy needs of Australians and the investigative needs of law enforcement agencies are best served through continuous ad-hoc amendments to the interception regime or whether the time is right to put in place a new interception framework that squarely focuses on the contemporary communications environment. The Department emphasised the need to strengthen the safeguards and privacy protections set out in the TIA Act but in a manner that considers the interception regime as a whole rather than any one aspect.

The PJCIS agreed, recommending, in its report tabled on 24 June 2013, at Recommendation 18, that the TIA Act be comprehensively revised with the objective of designing an interception regime that amongst other things, clearly protects the privacy of communications (at page xxviii of the Report).

The Department and relevant agencies are considering the recommendations in detail with a view to providing detailed advice to the Government about possible reform options.

2. ACCESS TO TELECOMMUNICATIONS DATA UNDER THE TIA ACT

2.1. WHAT IS TELECOMMUNICATIONS DATA?

Telecommunications data, also known as 'metadata', 'communications data' or 'non-content data' is not defined in the TIA Act, but the Department considers it to include:

- Information about the parties to a communication, or 'subscriber data', and
- Information that allows a communication to occur, or 'traffic data'.

A definition of telecommunications data reflecting the above was tabled by the Department during Senate Additional Estimates hearings in 2012, and subsequently provided to the PJCIS to assist it in its inquiry. A copy of this definition can be found at **Attachment A**.

The TIA Act also distinguishes between access to 'existing' telecommunications data, being data that a service provider already holds at the time they receive a request from an agency, and 'prospective' telecommunications data, which is any data that comes into existence after such a request is received.

2.2. DISTINCTION BETWEEN CONTENT AND TELECOMMUNICATIONS DATA

Telecommunications data does not include the content or substance of a communication, such as the content of an email, or data that would reveal the content of a communication, such as a person's web browsing history. Under the TIA Act, law enforcement and national security agencies can only intercept or access the content of a communication, or information that would reveal content, under a warrant issued by an issuing authority, being a judge or member of the Administrative Appeals Tribunal (AAT), or the Attorney-General.

The higher threshold for access to content reflects the greater privacy intrusion associated with covertly accessing the substance of a person's communications.

2.3. GENERAL PROHIBITION ON PROVIDERS DISCLOSING TELECOMMUNICATIONS DATA

Sections 276, 277 and 278 of the *Telecommunications Act 1997* (Telecommunications Act) create a general prohibition on providers (as well as number-database operators and emergency call persons) disclosing information or documents that relate to the content or substance of a communication, or personal affairs or particulars of their subscribers, including telecommunications data. The prohibition relevantly extends to employees and contractors of providers. In addition to limited exceptions provided in the Telecommunications Act, the TIA Act sets out the limited circumstances in which disclosure is authorised for law enforcement and national security purposes.

These circumstances recognise the valuable role telecommunications data plays in assisting agencies to investigate crime and national security matters. Australian law enforcement and national security agencies have been able to access telecommunications data under an authorisation issued by a senior officer for over 20 years. Provisions to this effect were included in the *Telecommunications Act 1991* and were replicated in the Telecommunications Act. The *Telecommunications (Interception and Access) Amendment Act 2007* transferred these provisions from the Telecommunications Act to Chapter 4 of the TIA Act.

3. IMPACT OF THE BILL ON INVESTIGATIONS AND PRIVACY

Requiring agencies to obtain a 'stored and other communications warrant' to access telecommunications data would involve three distinct changes to the current regime:

1. Law enforcement agencies would be required to obtain a warrant from a judge or member of the AAT, and ASIO would be required to obtain a warrant from the Attorney-General
2. The threshold for accessing existing telecommunications data by law enforcement agencies would be increased from 'the enforcement of the criminal law' to requiring agencies to be investigating a 'serious offence', as defined in the TIA Act, or an offence punishable by imprisonment for a period of at least three years, and
3. Law enforcement agencies and ASIO would be required to satisfy a significantly stricter legal test for obtaining a warrant.

The combined impact of these changes would likely be to considerably reduce the ability of law enforcement and security agencies to obtain telecommunications data. The implications of this change

would be complex. Telecommunications data is a vital investigative tool, particularly at the early stages of investigations where it is used to identify and obtain basic information about persons of interest, and to provide key evidence in support of warrant applications. Agencies may be able to substitute other, generally more intrusive powers for telecommunications data in some situations, however this is unlikely to fully offset the impact on their investigative capabilities. The likely result would be to limit the ability of law enforcement and national security agencies to progress many investigations beyond a preliminary stage.

The privacy implications of the Bill are also likely to be complex. On its face, the Bill appears to enhance privacy by limiting agencies' access to telecommunications data. The second order consequences of this change may adversely impact on privacy, however. This complexity is driven both by the Bill's likely operational implications, as well as how the Bill would interact with the existing, intricate provisions of the TIA Act.

The Department is of the view that enhancing privacy protection requires holistic reform of the interception regime that enables Government to:

- consider privacy in concert with operational implications
- reduce the complexity of the TIA Act to mitigate unintended, second order consequences, and
- allow users and participants, as well as the broader Australian community, to understand their powers, rights and obligations.

3.1. INVESTIGATIVE VALUE OF TELECOMMUNICATIONS DATA

Telecommunications data is not the only source of information available to law enforcement and national security agencies, however it is a critical investigative tool that agencies use in order to identify and prosecute criminals, and protect Australians.

Law enforcement and national security agencies can only access telecommunications data in limited circumstances. Authorising officers must be satisfied on a case-by-case basis that the disclosure of the information is reasonably necessary, and must consider the impact on privacy when making an authorisation. Telecommunications data is often used at the early stages of investigations to build a picture of a suspect and their network of criminal associates. It is also often combined with other information to enable agencies to more efficiently and effectively deploy their limited investigative resources.

It may not be commonly known that telecommunications data also plays an important role in protecting the privacy of innocent parties who come within the scope of an agency's investigation, by allowing the agency to rule them out from suspicion at an early stage and without having to resort to more privacy-intrusive investigative methods. For example, call charge records can show that a potential person of interest has had no contact with other members of a criminal syndicate, or was in fact at a different location at the time a crime was committed.

Telecommunications data is also frequently used to refine and direct the use of more intrusive investigative methods, such as telecommunications interception, avoiding unnecessary invasion of privacy. The ability of law enforcement and national security agencies to use telecommunications data at the early stages of an investigation also displaces the need for agencies to employ more intrusive alternative investigative methods to build a picture of a suspect and their network of criminal associates.

The Department is of the view that most viable alternative investigative methods involve a greater degree of privacy intrusion. The issue of whether other powers would be appropriate or adequate substitutes for telecommunications data is explored further at part 3.4, below.

Australian law enforcement agencies issued 293,501 telecommunications data authorisations in the 2011-12 financial year. This number reflects the utility of telecommunications data authorisations to

law enforcement agencies, but is also driven, in part, by its use at the early stages of an investigation. For example, it is often necessary for agencies to issue multiple authorisations for subscriber data to multiple providers simply to determine what phone, internet and email services a suspect is subscribed to. Reflecting this, over 85% of the requests made by the AFP for telecommunications data in the 2011-12 financial year were for subscriber data. Less than 15% of requests were for traffic data, such as a person's call charge records.

Several operational case studies involving the use of telecommunications data are included in this submission. Additional case studies are included at **Attachment B**.

Case study: ACC investigation of money laundering and drug importation

In February 2013, the ACC received information indicating Person A was processing illicit funds and potentially involved in money laundering. Enquiries revealed that Person A had not previously come to law enforcement attention.

The ACC made an authorisation for the subscriber details of Person A's mobile telephone number, which revealed that the phone account in fact belonged to Person B. Person B was suspected of arranging the importation and distribution of large quantities of illicit drugs. The ACC was then able to analyse relevant information based on the subscriber check, and identified a relationship between Person A and Person B. The ACC assessed that illicit funds being managed by Person A were likely derived from illicit drug sales conducted by Person B. Intelligence regarding this matter was referred to a Task Force for further investigation.

Without the ability to conduct a subscriber check at the initial stage of its investigation, the ACC was unlikely to have detected, or to have had the ability to investigate, this relationship.

3.2. USE OF TELECOMMUNICATIONS DATA IN NATIONAL SECURITY INVESTIGATIONS

Telecommunications data has proved critical in almost all ASIO investigations. ASIO uses telecommunications data to help it predict and prevent acts of terrorism, detect and thwart cyber-attacks, and counter espionage or illicit foreign interference.

In addition to the provisions of the TIA Act, ASIO's access to telecommunications data is governed by the Attorney-General's Guidelines. Pursuant to section 8A of the *Australian Security Intelligence Organisation Act 1979*, ASIO is required to comply with the guidelines in all of its operations. Section 10.4 of the Attorney-General's Guidelines requires *inter alia* that:

- any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence
- inquiries should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions, and
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.

As a result, telecommunications data helps ASIO avoid using more intrusive investigative techniques to pursue investigations (such as telecommunications interception).

ASIO also uses telecommunications data to help prioritise lead information to ensure investigations are pursued in the most effective and efficient way. This results in a better prioritisation of investigative resources and a maximum return on investment of government expenditure.

Access to telecommunications data by ASIO

Part 4-1 of the TIA Act empowers ASIO to authorise disclosure from telecommunications service providers of telecommunications data required for investigative purposes, so long as the authorising person is satisfied that the disclosure would be in connection with the performance by the Organisation of its functions.

ASIO is currently able to access telecommunications data held by service providers upon appropriate authorisation, provided the service providers have retained the data and it is in an accessible form.

ASIO has robust and thorough oversight and accountability arrangements for accessing and using telecommunications data. Accountability mechanisms are centred on an ongoing regime of inspections and inquiries by the Inspector-General of Intelligence and Security (IGIS). The IGIS is an independent statutory office holder who reviews the activities of Australia's intelligence agencies. The purpose of the IGIS is to ensure Australia's intelligence agencies act legally and with propriety, comply with ministerial guidelines and directives, and respect human rights. The Inspector-General has significant powers which include requiring the attendance of witnesses, taking sworn evidence, copying and retaining documents, and unescorted entry into an Australian intelligence agency's premises.

ASIO strictly adheres to the relevant legislation, the Attorney-General's Guidelines, internal policies and procedures and approval levels, all of which are open to scrutiny by the IGIS.

The IGIS reports on an annual basis on ASIO's access to and use of telecommunications data. In its 2011–12 Annual Report, the IGIS commented in relation to ASIO's use of prospective telecommunications data:

> *'During the reporting period we reviewed every request to renew (that is, continue) prospective telecommunications data collection to provide assurance that these authorities were renewed only where exceptional circumstances exist. I was satisfied that renewed requests for prospective telecommunications data were limited to those cases where reasonable alternatives did not exist.*
>
> *The inspections undertaken by OIGIS staff in 2011-12 revealed that all requests for prospective telecommunications data were endorsed at an appropriate senior level within ASIO. In the few instances where errors were made, these errors had already been identified by ASIO and appropriate remedial action taken. In circumstances where the reasons for the granting of the authorisation ceased to exist prior to the expiry of the authorisation, I found that ASIO consistently revoked the authorisation in a timely manner.*
>
> *Overall, we were satisfied that ASIO is using this method of inquiry in a suitable manner and that internal controls are well developed and appropriate.'*

3.3. USE OF TELECOMMUNICATIONS DATA IN WARRANT APPLICATIONS

The requirement under the Bill to obtain a stored and other communications warrant to access telecommunications data would remove the ability of law enforcement and national security agencies to access telecommunications data in the majority of cases.

As outlined in the introduction to part 3, above, the Bill would require agencies to satisfy strict legal tests in order to access telecommunications data under a stored and other communications warrant. The Department supports the requirement to meet a high legal standard in order to obtain a warrant authorising access to the content of a communication, but is of the view that such a standard would be impractical in relation to telecommunications data.

Telecommunications data provides vital evidence for agencies to be able to satisfy the legal test to obtain a warrant in most situations. Agencies would, in practice, rarely be able to meet the higher legal test without having first obtained telecommunications data. As a flow-on consequence, this would frequently prevent agencies from using any powers under the TIA Act, resulting in agencies 'going dark' and being unable to obtain any information about communications within criminal and terrorist groups.

By way of more detailed explanation, to obtain a stored or other communications warrant under section 116 of the TIA Act as amended by the Bill, law enforcement agencies would be required to demonstrate pursuant to subsection 116(1) *inter alia* that:

> (c) there are reasonable grounds for suspecting that a particular carrier
> (i) holds stored communications; or
> (ii) holds information or a document; or
> (iii) will hold specified information or specified documents that come into existence during the period for which the authorisation is in force;
>
> that the person has made, or that another person has made and for which the person is the intended recipient; and
>
> (d) information that would be likely to be obtained by accessing those stored or other communications under a stored or other communications warrant would be likely to assist in connection with
> (i) … the investigation by the agency of a serious contravention in which the person is involved …

For a law enforcement agency to satisfy paragraph 116(1)(c), the agency would be required to provide evidence demonstrating that it has reasonable grounds for suspecting that a carrier holds relevant telecommunications data. If an agency cannot demonstrate that the person even has an account with that provider, it will generally not be able to satisfy this test. At present, agencies would generally use subscriber data obtained under an internal authorisation to show that the person has an account with that carrier, which would satisfy the requirements of this paragraph. This is reflected in the fact that more than 85% of the AFP's requests for telecommunications data in 2011-12 financial year were for subscriber data, as outlined at part 3.1, above. Without access to such data under an internal authorisation, it will be difficult for an agency to actually demonstrate that a particular carrier holds relevant telecommunications data. The ability of agencies to use alternative powers in lieu of telecommunications data is explored further in part 3.4, below.

Similarly, in order to satisfy paragraph 116(1)(d), law enforcement agencies would be required to demonstrate that the telecommunications data, such as the records of whom a person has called on the phone, would be likely to assist with their investigation. If an agency cannot demonstrate that the phone is, in fact, being used to call criminal associates it will again be difficult to meet the strict warrant test that such data 'would be likely to assist' in the investigation. Traffic data, such as a person's call charge records, would ordinarily be essential evidence for this paragraph.

As such, requiring agencies to meet the stricter legal test to obtain a stored and other communications warrant to access telecommunications data would, in many cases, be an insurmountable barrier and would stall investigations at their early stages. The Bill would, therefore, significantly undermine the investigative capabilities of law enforcement and national security agencies by preventing them from accessing telecommunications data and, as a direct consequence, from utilising other telecommunications interception powers.

Access to telecommunications data by ACLEI

ACLEI makes use of telecommunications data in its corruption investigations when the allegations under investigation also constitute the potential commission of criminal offences. The power to make an authorisation is restricted to higher-level staff members who have an active role in managing and directing ACLEI's investigative work.

ACLEI has had particular success using telecommunications data to identify, trace and explore the extent of corruption networks within law enforcement and the linkages of such networks to organised crime. This material is also often used to direct the appropriate allocation of investigative resources (thereby assisting with the efficiency of investigations), and as supporting evidence for warrant applications for the use of more-intrusive investigative tools, namely telecommunications interception or surveillance devices.

3.4. SUBSTITUTION OPTIONS

As noted at part 3.1, above, telecommunications data is one source of information available to agencies. Law enforcement and national security agencies have access to a range of powers, such as search warrants, surveillance devices and telecommunications interception. By restricting the ability of agencies to access telecommunications data, the Bill may compel agencies to resort to more privacy-intrusive investigative methods to collect what is, frequently, preliminary information for an investigation.

Most alternative investigative powers available to agencies are more privacy intrusive than accessing telecommunications data. For example, the use of a listening device in a person's house or car would be significantly more privacy-intrusive than accessing a person's call charge records from their provider.

Such powers are not appropriate substitutes for telecommunications data, however, as they would be both disproportionate to and inadequate for agencies' investigative needs.

Additionally, the alternative investigative powers available to agencies would, at best, only partially offset the harm to agencies' investigative capabilities from reduced access to telecommunications data. As such, the Bill would compromise the overall investigative capabilities of law enforcement and national security agencies.

For example, an agency might attempt to use physical surveillance or a surveillance device to determine which provider a person uses and with whom they communicate. Such methods would, however, risk compromising a covert investigation if the surveillance, or the installation, maintenance or removal of the surveillance device, was in any way observed or detected. In this fashion, the use of more overt powers is often unsuitable, particularly at the very early stages of an investigation when telecommunications data is most frequently used. Similar reasoning would apply to the use of a search warrant or to questioning individuals.

Case study: Investigations into sophisticated serious and organised criminal groups

In recent decades, information and communication technologies have diversified at a staggering rate. The growth and rapid change in telecommunication technologies, global participants and consumer behaviours have created a more diverse and dynamic telecommunications environment. As communications and commercially available encryption services continue to evolve, national security and law enforcement agencies confront persistent and growing challenges in obtaining lawful access to telecommunication interception.

The ACC has observed an increasing trend in the use of encrypted or secure communications by serious and organised crime targets to deliberately impede the ability of law enforcement agencies to lawfully intercept content. Indeed, traditional telecommunications interception does not provide the same information and intelligence as it did ten years ago.

Therefore there has been a shift to better utilise less-intrusive information sources to supplement traditional law enforcement and national security tools. Telecommunications data is one such example of a less-intrusive information source that can effectively assist investigations by identifying links and networks. As telecommunications data is a less-intrusive source of information, does not contain private conversations, does not by itself incriminate nor entrap, it has become an essential source of information for law enforcement and national security agencies.

3.5. Access to Telecommunications Data

Part 4.1 of the TIA Act sets out the circumstances in which 'enforcement agencies' may authorise providers to disclose telecommunications data. Enforcement agencies include all interception agencies and Commonwealth, State or Territory agencies whose functions include administering the criminal law, a law imposing a pecuniary penalty or a law relating to the protection of the public revenue.

This includes Commonwealth and State government departments and agencies such as Centrelink, many local government authorities, and bodies such as the Royal Society for the Prevention of Cruelty to Animals (which plays a role in investigating assaults and other legislated crimes against animals).

The wide range of agencies that can be considered to be enforcement agencies was an issue referred to and considered by the PJCIS. The Department suggested in its Submission that privacy interests could be strengthened if only agencies that have a demonstrated need to access communications information were eligible to do so. The PJCIS broadly agreed with this approach, noting at paragraph 2.54 that it was satisfied that 'access to telecommunications data for serious crime and threats to security is justified. Access for agencies not enforcing the criminal law or investigating security threats should be subject to further review.'

Reviewing the range and types of agencies that can be considered to be an enforcement agency offers more rigorous privacy protection than altering the methodology through which the same number of agencies can access information.

Access to telecommunications data by the AFP

Authorisations for access to telecommunications data by the AFP may only be made by sworn officers of the rank of Superintendent or above, and are made on a case-by-case basis for individual investigations.

The AFP is held accountable for its access to and use of telecommunications data by the ministerial reporting requirements mandated by the TIA Act and the admission at trial of evidence collected as interception product or telecommunications data. In addition, all requests for telecommunications data made by the AFP are reported to the Parliament in the Attorney-General's Annual Report on the TIA Act, which is publicly available.

The AFP is also accountable to the Commonwealth Ombudsman for the use of its powers under the TIA Act more generally, both under specific provisions of the TIA Act and by virtue of the Ombudsman own motion power to inspect any administrative process of the AFP. The Ombudsman has not reported any adverse findings in relation to the AFP's practices under the TIA Act to the Attorney-General.

Access to prospective telecommunications data is generally more privacy intrusive than access to existing telecommunications data as it provides near-real-time information about a person's communications. In the case of data associated with mobile phones, this can allow agencies to track the general, rather than the specific, location of a person based on which cell towers are being used. For example, if a suspect was having a meeting at the Manuka shops in Canberra, cell tower records obtained under a prospective data authorisation would show that a person's phone was connected to a cell phone tower in the vicinity of Manuka. It would generally not, however, be sufficiently precise to place the person in a particular restaurant, or even necessarily on a particular block.

Reflecting the greater privacy intrusion involved, access to prospective telecommunications data for criminal investigations is only permitted for the purpose of investigating a serious offence, or an offence carrying a penalty of imprisonment for at least three years and is restricted to 'criminal law enforcement agencies',[63] which is a significantly narrower range of enforcement agencies.

[63] The Australian Federal Police, a Police Force of a State, the Australian Commission for Law Enforcement Integrity, the Australian Crime Commission, the Crime Commission (NSW), the Independent Commission Against Corruption (NSW), the Police Integrity Commission (NSW), the Independent Broad-based Anti-corruption Commission (Vic), the Crime and Misconduct Commission (Qld), the Corruption and Crime Commission (WA), the Independent Commissioner Against Corruption (SA), or an prescribed authority established by or under a law of the Commonwealth, a State or a Territory.

Access to telecommunications data by the ACC

The ACC is Australia's national criminal intelligence agency. It is a statutory authority with primary responsibility for combating nationally-significant organised crime in Australia. It draws on its unique investigative capabilities to provide government with an independent view of the risk of serious and organised crime.

Access to telecommunications data is a critical investigative tool for the ACC. The majority of ACC operations are assisted by some form of telecommunications data. Each request for access must be specifically justified and is carefully considered by a senior ACC delegate, who must consider the impact on privacy. The applicant must specify the reason for the request, the particulars of the offence and identify the Determination under which the request is sought. A Determination is an ACC Board-authorised investigation or intelligence operation that the Board has determined is a 'special investigation' or 'special operation' because traditional law enforcement methods are likely to be—or have been—ineffective.

The ACC has oversight and accountability arrangements that govern the access and use of telecommunications data. The ACC is accountable to a number of well-established external scrutiny mechanisms, including to the Commonwealth Ombudsman, who has an own motion power to inspect any administrative process of the ACC.

The Ombudsman has not made any official recommendations over the past three years about the ACC's compliance with the TIA Act and has remarked favourably on the strong compliance mechanisms in place within the ACC. The oversight provided by the Ombudsman is thorough, objective and independent, and provides avenues for complaints and for addressing natural justice concerns.

3.6. VOLUNTARY DISCLOSURE OF TELECOMMUNICATIONS DATA BY SERVICE PROVIDERS

The Bill would repeal sections 174 and 177 of the TIA Act, which permit providers to voluntarily disclose telecommunications data to ASIO and enforcement agencies, respectively. At present, these provisions permit providers to voluntarily disclose telecommunications data to enforcement agencies if the disclosure is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for protecting the public revenue. Similarly, providers may voluntarily disclose telecommunications data to ASIO if the disclosure is in conjunction with ASIO's functions. The TIA Act specifically prohibits the voluntary disclosure of information where an agency requests the information to be disclosed.

Subsections 313(1) and (2) of the Telecommunications Act require providers to do their best to prevent their networks and facilities from being used in, or in relation to, the commission of criminal offences. The Department notes that these provisions are distinct from subsection 313(3), which requires providers to provide agencies with 'reasonably necessary assistance' in enforcing the criminal law (amongst other things) and which has been the subject of recent media reporting in relation to web site blocking.

As noted at part 2.3, above, sections 276, 277 and 278 of the Telecommunications Act would ordinarily prohibit providers from disclosing any information or document about a communication or their subscribers, including telecommunications data. The voluntary disclosure provisions assist providers to meet their legal obligations under subsections 313(1) and (2) of the Telecommunications Act by reporting instances where they believe their networks are being used for criminal purposes to the relevant authorities. In particular, these provisions allow providers to notify authorities of a range of cybercrimes that are likely to be detected during their normal network-management processes, such as spam, child exploitation material, hacking attempts and other cyber-attacks.

Removing the ability of providers to voluntarily disclose telecommunications data to law enforcement and national security agencies would undermine the ability of agencies to detect, investigate, disrupt and prosecute a range of cybercrimes that are most likely to come to the attention of providers.

Additionally, the Bill would increase the regulatory burden on those providers by removing a method which assists them to meet their legislative obligations under the Telecommunications Act, notifying the relevant authorities of a suspected crime. Providers would instead be required to adopt alternative methods to discharge their duties, which are likely to be more onerous for private companies to undertake.

Access to telecommunications data by Customs and Border Protection

Telecommunications data is a valuable source of information that contributes significantly to the Australian Customs and Border Protection Service operational, investigative and intelligence capability to manage the security and integrity of Australia's border through detecting, deterring or disrupting criminal border activity.

Approval of access to telecommunications data is limited to certain officers who have been granted authorisation by the CEO as an authorised officer for the purposes of the TIA Act. Access to telecommunications data is limited to a small telecommunications processing team and the senior officer or Manager of that team grants approval on a case-by-case scenario after satisfying stringent internal policy and procedures and the legislation governing such requests including the TIA Act, including considering the impact on privacy, to ensure that disclosure of telecommunications data is in accordance with the powers granted to Customs and Border Protection as an enforcement agency. Customs and Border Protection applies a high standard of scrutiny before submitting requests for access to telecommunications data including local processes of ensuring the information cannot be sought through other means prior to accessing telecommunications data and that the offences being investigated are a priority for the Service. As an enforcement agency, Customs and Border Protection accesses telecommunications data only for purposes in accordance with the TIA Act and which are reasonably necessary for the investigation of an offence against a law of the Commonwealth, a State or Territory with sufficient Customs and Border Protection relevance.

Customs and Border Protection is transparent and accountable for all requests for telecommunications data and is compliant with the Commonwealth Ombudsman's general auditing processes. Customs and Border Protection also fulfils all requirements of s 186 of the TIA Act, where the CEO must provide the Minister and Parliament with an annual report of the number of authorisations made by the Service which is available for media and public scrutiny.

4. Report of the Inquiry into Potential Reforms of Australia's National Security Legislation

As mentioned above, the former Attorney-General asked the PJCIS to inquire into a number of potential reforms to Australia's national security legislation, including to the TIA Act. In the course of its inquiry, the PJCIS received 240 submissions and 27 exhibits and three private briefings, and held six public hearings, three classified hearings and one private hearing.

The PJCIS tabled the report of its inquiry on 24 June 2013. The PJCIS's report contains 43 recommendations, 20 of which relate to the telecommunications interception regime. Three of these recommendations are directly relevant to the subject matter of the Bill, namely:

- that the Department review the threshold for access to telecommunications data with a view to reducing the number of agencies able to access telecommunications data (Recommendation 5)

- that the Department examine the standardisation of thresholds for accessing the content of communications (Recommendation 6), and
- that the TIA Act be comprehensively revised (Recommendation 18).

The Government has committed to considering the PJCIS's recommendations before making a decision about what, if any, legislative amendments to the TIA Act will be progressed. The Department and relevant agencies are currently considering the recommendations in detail with a view to providing detailed advice to the Government about possible reform options.

5. RESOURCING IMPLICATIONS

Irrespective of the threshold or legal standard for accessing telecommunications data, warrant applications are resource intensive, both for the applicant agencies and for the issuing authorities hearing the applications, being members of the judiciary acting *in personam*, members of the AAT and the Attorney-General.

In the 2011-12 financial year, law enforcement agencies made 293,501 authorisations for access to existing telecommunications data for the purpose of enforcing the criminal law. The Department acknowledges that the difficulties associated with meeting threshold requirements without pre-existing telecommunications data, as outlined at part 3.3, above, combined with internal resource limitations, would likely result in only a proportion of these authorisations being re-made as warrant applications.

The Department notes, however that each authorisation must be justified on a case-by-case basis as being 'reasonably necessary', and that the Bill will not remove the operational imperatives for agencies to access telecommunications data. As such, the Department considers that agencies will find it reasonably necessary to re-make a significant proportion of their authorisations as warrant applications under the Bill, resulting in a substantial and sustained increase in the number of warrant applications.

For example, in the 2011-12 financial year, the ACC made 13,518 authorisations to access telecommunications data. During that same period the ACC made 143 applications to the AAT for telecommunications interception warrants and 8 applications for stored communications warrants. Given that the ACC's primary responsibility is combating serious and organised crime, the Department considers that it is likely that a substantial proportion of the ACC's authorisations would be re-made as warrant applications, subject only to internal resource limitations.

Constrained resources within law enforcement and national security agencies and for issuing authorities would therefore likely result in the warrant application process becoming an investigative 'bottleneck', limiting the ability of agencies to effectively investigate serious crime and national security matters.

Additionally, given the way in which telecommunications data is used in investigations, the time necessarily involved in preparing, reviewing and granting a warrant application to access such data would:

- significantly delay and, in some circumstances, undermine law enforcement and national security investigations
- impede operational activity, including the prevention of criminal acts, and
- divert scarce investigative resources during the critical, initial stages of an investigation.

Investigative resources would also need to be diverted to less time-efficient investigative mechanisms, such as physical surveillance, to assist with grounds for the warrant application.

The requirement to obtain a warrant for telecommunications data would make agencies dependent on external processes from an early point in the investigation. This dependency would undermine the ability of agencies to respond rapidly and flexibly as an investigation develops.

The Department is of the view that, by limiting the ability of agencies to access telecommunications data, the Bill would have a secondary effect of reducing the efficiency of issuing authorities, and law enforcement and national security agencies. Additionally, the ongoing financial and resource investment necessary to maintain an effective warrant regime for telecommunications data that maintains public safety and security, or at least limits its degradation to a level acceptable to government, would be unsustainable.

6. CYBERCRIME INVESTIGATIONS

Amending the TIA Act to require agencies to obtain a stored communications warrant to access telecommunications data would have a particularly significant impact on cybercrime investigations and would place Australia in breach of its international obligations.

6.1. USE OF TELECOMMUNICATIONS DATA IN CYBERCRIME INVESTIGATIONS

Cybercrimes, by definition, have a limited physical footprint. Telecommunications data is, therefore, essential for identifying, investigating, preventing and prosecuting cybercrimes. For example, telecommunications data is critical for tracing cyber-attacks across networks and, in particular, for linking IP addresses to a particular subscriber.

Providers typically store IP-based telecommunications data only for a very limited period of time, if at all, as commercial billing practices for IP-based services are generally volume-based: billing is based on the total volume of information uploaded and downloaded, not on whom a person was communicating with. The delay necessarily associated with preparing a warrant application for telecommunications data, or even making an emergency application, would give rise to a real risk that critical IP-based telecommunications data would have been purged from a provider's systems by the time a warrant was issued and executed, frustrating cybercrime investigations.

Case study: Use of telecommunications data in a major online child abuse investigation

In mid-2008, the AFP began one of the largest investigations ever conducted into online child abuse. During the course of the investigation, 141 people were arrested, 400,000 images were seized, and, most importantly, four children were removed from harm. Prompt and effective access to telecommunications data was essential to the success of this investigation.

It is important to appreciate the context in which access to telecommunications data occurs in operations of this type. Online child sexual exploitation is a technology-dependent crime type. The initial referral to the AFP, or to any law enforcement agency, may only indicate that a particular IP address accessed a website containing child exploitation material at a particular time and date, and that the IP address originated from Australia. Telecommunications subscriber data can be used as a starting point to identify the person using the IP address at the time the exploitation material was accessed. Information about an IP address that has uploaded child exploitation material can also be used to commence victim identity and rescue operations.

6.2. INTERNATIONAL COOPERATION TO COMBAT CYBERCRIME

Cybercrime is an inherently borderless crime. High-speed telecommunications networks span the globe, revolutionising global communications but also allowing criminals to perpetrate cybercrimes across borders with ease. The ability and willingness of law enforcement agencies to effectively share telecommunications data, such as the IP address behind a cyber-attack, with their counterparts in other jurisdictions in a timely fashion is, therefore, fundamental to most cybercrime investigations.

The TIA Act allows the AFP to access telecommunications data on behalf of a foreign law enforcement agency and to disclose those communications, or other lawfully accessed communications data, to a foreign law enforcement agency.

The TIA Act places additional controls over accessing and disclosing telecommunications data for the purpose of providing assistance to foreign law enforcement agencies. The AFP must not disclose existing telecommunications data to a foreign agency unless it is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of that foreign country, and that the disclosure is appropriate in all of the circumstances.

The Attorney-General must authorise access to, and the disclosure of prospective telecommunications data to assist foreign law enforcement agencies under the *Mutual Assistance in Criminal Matters Act 1987*, reflecting the more privacy intrusive nature of this power. Access to prospective telecommunications data is only permitted for the purpose of investigating a foreign offence carrying a penalty of imprisonment for at least three years and, again, the AFP must also be satisfied that disclosure of the data would be appropriate in all the circumstances.

The Bill proposes to remove the ability of Australian law enforcement agencies to access and share telecommunications data with their foreign counterparts. Such a step would significantly undermine the ability of Australian agencies to share information with foreign agencies for the purpose of progressing Australian investigations. It would also limit the ability of Australian agencies to assist foreign jurisdictions with their own investigations, which would place the goodwill and cooperation of such agencies at risk.

6.3. INTERNATIONAL LEGAL OBLIGATIONS

Australia is a party to the Cybercrime Convention, which is the leading international instrument on combatting cybercrime.

Articles 14 and 18 of the Convention require Australia to *inter alia* ensure that agencies are able to access telecommunications data to '[collect] evidence in electronic form of a criminal offence'. Australia complies with these Articles by permitting enforcement agencies to access telecommunications data 'for the enforcement of the criminal law'.

Additionally, Articles 29 and 30 of the Convention requires Australia to expeditiously preserve and disclose telecommunications data at the request of another Convention country for the purpose of a foreign criminal investigation or proceeding. Division 4A of Part 4 of the TIA Act contains provisions that allow Australia to comply with these Articles.

By restricting access to telecommunications data to offences carrying a penalty of three years imprisonment, and by repealing Division 4A of Part 4, thereby removing the ability of Australian law enforcement agencies to share telecommunications data, the Bill would place Australia in breach of its international obligations under the Cybercrime Convention.

7. DRAFTING ISSUES

The Bill, as drafted, is likely to produce a number of unintended consequences. Many of these consequences are contradictory or mutually exclusive, but represent grave risks to privacy, public safety and security.

7.1. 'CREATION' OF TELECOMMUNICATIONS DATA

The Bill fundamentally misunderstands the nature of telecommunications data and, as a consequence, would prevent law enforcement agencies from accessing almost any useful information about a suspect's communications under a warrant.

Section 3 of the Bill would replace section 117 of the TIA Act. The new section 117 would authorise law enforcement agencies to access, under a warrant, telecommunications data 'made by the person in respect of whom the warrant was issued' or 'made by another person in circumstances where the intended recipient is the person in respect of whom the warrant was issued'.

Telecommunications traffic data includes data such as billing and cell tower records which are created by carriers and carriage service providers as part of their business and technical processes. It is not 'made by' the person using the phone or writing the email. Nor is it necessarily ever sent to them. It is, in essence, the by-product of a communication. Even the majority of subscriber data will in fact be 'made by' employees of a provider who perform the physical data-entry when setting up a new customer's account.

By conflating the concept of telecommunications data with content, the Bill would prevent law enforcement agencies from accessing the vast majority of telecommunications data, even if the agency were able to obtain a warrant.

7.2. PROSPECTIVE DATA AUTHORISATIONS

As outlined at part 2.5, above, prospective data authorisations allow criminal law enforcement and national security agencies to access telecommunications data, including general location data, in near-real-time. The use of this power has the potential to be more privacy-intrusive than access to existing or historic records, and so is restricted to a more limited range of agencies that have a demonstrated need to access such data in near-real-time.

The Bill would repeal sections 176 and 180 of the TIA Act and require law enforcement agencies to obtain a stored and other communications warrant to access prospective telecommunications data. This would create two unintended and contradictory consequences.

First, pursuant to section 116 of the TIA Act as amended by the Bill, stored and other communications warrants would be available to all 'enforcement agencies'. This would expand the range of agencies permitted to access prospective data to include any agency whose functions include administering a law imposing a pecuniary penalty or relating to the protection of the public revenue, including bodies such as the RSPCA and certain local government authorities.

Second, stored and other communications warrants, as provided for under the Bill, are not in fact capable of authorising access to prospective telecommunications data. Pursuant to section 119 of the TIA Act as amended by the Bill, a stored and other communications warrant would cease to be in force the moment it was executed on a provider. Enforcement agencies would not be able to actually obtain prospective telecommunications data under these warrants as the authority would cease the moment the warrant was executed. As such, enforcement agencies would only be able to obtain real-time data under a live interception warrant, which is only available for the investigation of a 'serious offence', as defined in the TIA Act.

7.3. INCONSISTENCY BETWEEN CRIMINAL, PECUNIARY PENALTY AND REVENUE INVESTIGATIONS

The Bill requires enforcement agencies to obtain a warrant to access telecommunications data for the purpose of enforcing the criminal law, but not for enforcing a law imposing a pecuniary penalty or the protection of the public revenue. This approach is inconsistent with the recommendations of the PJCIS.

It is also unlikely to achieve the policy objective of the Bill, namely to require agencies to obtain a warrant to access telecommunications data for criminal investigations, as it creates a significant 'loophole' for law enforcement agencies.

First, many enforcement agencies have functions that span the criminal law, pecuniary penalty provisions and revenue protection. The Bill would, on its face, introduce an inconsistent standard based on the nature of an investigation or the available penalty, rather than the gravity of the conduct concerned. This is inconsistent with recommendation 15 of the PJCIS's report, which recommended that the TIA Act use the 'gravity of conduct… as the threshold on which access is allowed.'

Second, section 4B of the *Crimes Act 1914* allows the court to impose a pecuniary penalty for any offence against a law of the Commonwealth that is punishable by imprisonment only. As such, the Bill may contain a significant loophole whereby enforcement agencies could continue issuing existing telecommunications data authorisations under section 179 on the basis that pecuniary penalties are available for all criminal offences.

8. CONCLUDING REMARKS

The Department supports modernising and strengthening the safeguards, privacy protections, and accountability and oversight mechanisms within the TIA Act, while balancing agencies' ability to effectively and efficiently obtain intelligence, and investigate and prosecute criminal activity. It is the Department's view that the Bill does not find that balance and would have a significant impact on community expectations that criminal activity would be investigated and prosecuted, and that security be safeguarded.

Telecommunications data is a vital investigative tool for Australian law enforcement and national security agencies. It will generally be difficult to meet the threshold required to obtain a warrant at the initial stages of an investigation, which is where access to telecommunications data is most frequently sought. The likely result would be to limit the ability of law enforcement and national security agencies to progress many investigations beyond a preliminary stage. This will be particularly true for cybercrime and high-tech crime investigations which, by definition, rely more heavily on telecommunications data.

The privacy implications of the Bill are complex. On the face of it, the Bill appears to enhance privacy by limiting the ability of agencies to access telecommunications data, however the second order consequences of this change could have negative impacts, including by:

- Leading to agencies to employ more intrusive powers more frequently
- Reducing the ability of agencies to exclude innocent third parties from investigations in a timely fashion, and
- Reducing the ability of agencies to combat serious crime, with attendant consequences for the privacy of the victims of such crime.

The Bill would also place Australia in breach of its international legal obligations and, in its current form, contains significant drafting flaws which have the potential to gravely undermine privacy, public safety and security.