Australian Government

Attorney-General's Department

National Security Law & Policy Division

14/14457-04

16 January 2015

Dr Anna Dacre
Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Dear Dr Dacre

Departmental Submission and Proposed Data Retention data sets

I enclose the Department's submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill). I also attach the related Privacy Impact Assessment, which may assist the PJCIS in its consideration of the Bill.

The Bill contains measures that will require Australian telecommunications service providers to retain certain telecommunications data for a period of two years. In addition to the Bill, the Attorney-General also referred the proposed data set to the Committee. The data set is also available at <www.ag.gov.au/nationalsecurity/dataretention>. The proposed data set is based on current, best-practice retention practices within the telecommunications industry and does not require the retention of telecommunications data that is not currently retained by at least one provider.

The Bill includes a regulation-making power to prescribe the data that is to be retained. At its hearing on 17 December 2014 the Committee enquired as to the status of the proposed data set, and particularly how to treat the data set referred by the Attorney-General in light of the subsequent recommendations for amendment by the Implementation Working Group (IWG).

The IWG is a joint Government-industry executive level forum established to support continued engagement between the telecommunications industry and the Government on implementation of the data retention obligation. The IWG's terms of reference invited the IWG to consider whether further refinement could be made data set. The Government envisaged that the IWG's views, assisted by experts and representing a consensus from both agency and industry representatives, may assist the PJCIS's inquiry into the Bill and the proposed data set.

The IWG report is intended to assist the Committee's consideration of the proposed data set rather than provide a replacement. The Government welcomes the Committee's views on the data set as referred.

Yours sincerely

Anna Harmer
Acting First Assistant Secretary

Australian Government
Attorney-General's Department

January 2015

Submission

Parliamentary Joint Committee on Intelligence and Security

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

[This page intentionally left blank]

Table of Contents

Introduction **5**
The need for data retention 5
Overview of this Submission 7

Overview of the challenge and potential solutions **10**
Overview of the investigative environment 10
Challenges facing Australia's law enforcement and national security agencies 12
Alternatives to mandatory data retention 15
Operation of Schedule 1 of the Bill 22
Application of data retention obligations 23
Data retention obligations—the dataset 24
Retention periods 30
Use of telecommunications data by service providers 33
Implementation arrangements 33
Enforcement 35
Review of the operation of the scheme by this Committee 36
Annual reporting on the operation of the scheme by the Attorney-General 36
Information security 37
Existing information security frameworks 37
Telecommunications Sector Security Reforms 38
International comparisons 38

Restricting access to stored communications and telecommunications data **41**
Current framework for agency access 41

Oversight **50**
Current oversight of TIA Act powers 50
Amendments - new Ombudsman oversight 51

Appendix A—Summary of data retention and access arrangements in Western countries **55**

Appendix B—Number of data authorisations from *Telecommunications (Interception and Access) Act 1979 Annual Report 2012—13* **57**

Appendix C—Department's submission to the Senate inquiry into the *Telecommunications Amendment (Get a Warrant) Bill 2013* **578**

[This page intentionally left blank]

Introduction

The Telecommunications (Interception and Access) Act 1979 (the TIA Act) allows a limited number of Australian law enforcement and national security agencies to access the content of communications. In addition, the Act enables access to non-content telecommunications data to support the enforcement of the criminal law, the enforcement of a pecuniary penalty and the protection of public revenue. The Act provides Australia's law enforcement and anti-corruption agencies with investigative tools necessary to protect the safety and security of Australians, and uphold the rule of law.

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) will amend the TIA Act to require telecommunications service providers to retain a limited subset of telecommunications data essential to support law enforcement and security investigations. The Bill aims to ensure Australia's law enforcement and national security agencies retain their investigative capabilities in the face of rapid technological developments.

The need for data retention

As modern communications technologies have become increasingly embedded in daily life, they have also become an essential part of the modus operandi of serious criminals and persons engaged in activities prejudicial to security. By nature, electronic communications do not leave a physical footprint, allowing individuals and groups to plan and carry out such activities without risk of detection via 'traditional' investigative techniques. The records kept by telecommunications companies about the services they have provided (telecommunications data) are a vital source of information for agencies to detect and investigate crime and threats to national security.

Telecommunications data is critical to the investigation of almost any criminal activity, serious or otherwise, and almost any activity prejudicial to security that has been facilitated, enabled or carried out via communications technology. For online investigations, telecommunications data is, in many cases, the primary form of information used by law enforcement agencies to identify, investigate, prevent and prosecute these serious crimes and threats to national security. It is used in almost all national security investigations conducted by the Australian Security Intelligence Organisation (ASIO), including almost all counter-terrorism, espionage and intelligence investigations, and all cyber-security investigations.

Telecommunications data can provide important leads for agencies, including evidence:

- of connections and relationships between persons of interest
- of suspects' movements and behaviours
- of events immediately before and after a crime, and
- to exclude people from suspicion.

Telecommunications data is also foundational information required as a necessary precondition to more intrusive investigative tools such as access to stored communications and telecommunications interception. Conversely, it is always desirable to rule innocent parties out from suspicion as early as possible, both to prevent any unnecessary intrusion on their privacy, and to ensure that scarce investigative resources are used efficiently. While all investigative techniques involve some degree of intrusion, the use of telecommunications data is one of the least privacy intrusive investigative tools available to agencies.

Australia's law enforcement and national security agencies are facing several challenges which have increased their need to reliably access telecommunications data. These include:

- a long-term decline in and significant industry inconsistency in the retention of relevant telecommunications data
- a long-term decline in agencies' ability to lawfully access the content of communications under warrant has been a trend, driven by technological change and the globalisation of telecommunications, requiring them to increasingly rely on alternative investigative techniques, including access to telecommunications data, and
- an increasingly high-risk operational environment, caused in part by the increased risk of a terrorist attack.

Despite this increasing reliance on telecommunications data, Australia's telecommunications industry is not subject to any obligation to retain the information for the purpose of supporting law enforcement and security functions. Rapid changes to the technologies and business practices of the Australian telecommunications industry are resulting in providers keeping fewer records, and keeping those records for shorter periods. In June 2013 the PJCIS concluded that these changes are resulting in 'an actual degradation of the investigative capabilities of the national security agencies, which is likely to accelerate in the future.'

Attempts by Government and agencies to address the declining availability of telecommunications data with industry have had limited success. Without legislative obligations, the Government does not have the ability to prevent changes in retention practices based on commercial decisions that significantly degrade agencies' investigative capabilities. As a result, agencies have previously submitted to the PJCIS that 'without legislated data retention obligations the degradation of investigative capability will be significant.'

There are no practical alternatives to a legislated mandatory data retention scheme. International counterparts have considered the expansion of existing 'quick freeze' preservation notices to cover non-content data as an alternative to data retention. Unfortunately, service providers cannot preserve information that no longer exists. Thus, a preservation notice scheme cannot assist where record-keeping practices are inadequate. The purpose of data retention is to introduce a consistent industry standard to ensure that certain limited types of telecommunications data are consistently available.

The introduction of a mandatory data retention scheme is consistent with international approaches to these challenges. More than 35 Western countries have legislated data retention schemes. Many of these countries implemented data retention laws in accordance with the former European Union Data Retention Directive. Others, such as Switzerland and the United States, have implemented data retention laws independently and, in the case of Switzerland, have recently increased the retention period based on their operational experience.

The Department acknowledges that the Court of Justice in the European Union (ECJ) declared the Data Retention Directive invalid. The ECJ found data retention itself was not necessarily a breach of human rights; however the Directive itself was invalid because it lacked adequate privacy safeguards. The Data Retention Bill has been carefully drafted to avoid these shortcomings. For instance, the Bill entirely exempts a large number of communications services where the privacy or compliance impact would be disproportionate to the investigative benefit. Likewise, the circumstances in which agencies may access, use and disclose telecommunications data, and impose criminal penalties for the misuse of such information are strictly controlled under existing legislation.

Overview of this Submission

Part 1 provides an overview of the challenge facing law enforcement and national security agencies and explores the need for an industry-wide mandatory data retention scheme. It then examines key elements of Schedule 1 of the Data Retention Bill, including:

- an explanation of the proposed dataset and retention periods
- the application of the data retention obligations
- implementation arrangements
- exemptions from data retention obligations, and
- enforcement arrangements.

The data retention obligation has been strictly limited to data that is vital to law enforcement and national security investigations, and has been informed by considered advice from both agencies and the telecommunications industry. The Bill will impose a minimum obligation on telecommunications service providers to keep a limited set of telecommunications data. The Bill requires the retention of certain subscriber records for the life of the account plus two years, and other types of data listed in the dataset to be retained for two years after they come into existence.

Data retention obligations will apply to communication services provided by Australian carriers, carriage service providers and internet service providers, subject to a number of substantial exceptions and an exemptions regime. The exceptions and exemptions will ensure that data retention obligations are tailored having regard to both law enforcement and security imperatives as well as compliance cost and related industry considerations. This flexibility ensures that industry is not unduly burdened and individual privacy is protected.

The Bill recognises that mandatory data retention will have a varying impact on industry. Industry will be able to seek approval of an individualised implementation plan to reach full compliance 18 months from the commencement of the mandatory data retention obligation.

Schedule 1 of the Bill also permits service providers to seek exemptions from data retention obligations having regard to a range of factors including the interests of law enforcement and national security, the costs of compliance and any alternative strategies for data retention. This mechanism provides the flexibility to modify the data retention obligation having regard to the need to support agencies' capabilities while being mindful of the compliance impact on the telecommunications industry.

Part 2 outlines proposed amendments to alter the range of agencies empowered to exercise certain powers under the TIA Act. Schedule 2 of the Bill will limit the range of agencies and bodies that can access telecommunications data or stored communications by amending the definitions of 'enforcement agency' and 'criminal law-enforcement agency' in the TIA Act.

Part 3 examines the oversight and accountability arrangements proposed in the Bill. The Commonwealth Ombudsman will be granted new powers to comprehensively assess agency compliance with all of an enforcement agency's (or criminal law-enforcement agency's) obligations under Chapters 3 and 4 of the TIA Act, including use of and access to telecommunications data.

There is currently no independent oversight of the use of, and access to, telecommunications data by enforcement agencies. The oversight model contained in the Bill will empower the Commonwealth Ombudsman to assess agency compliance in relation to their obligations under the TIA Act and provide a higher level of guidance in meeting those requirements. The model supports effective oversight among agencies by providing precise compliance obligations, more consistent reporting on access of telecommunications data and more accurate statistics for annual reporting and other audit-related purposes.

The Bill has been developed with a view to ensuring it enables Australia's law enforcement, anti-corruption and national security agencies to investigate serious wrongdoing while being mindful of the compliance burden on industry, providing appropriate oversight and accountability and the protection of rights and freedoms.

[This page intentionally left blank]

1. Overview of the challenge and potential solutions

Schedule 1 of the Bill requires certain telecommunications service providers to keep a limited set of telecommunications data.

Overview of the investigative environment

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

Modern communications technologies have revolutionised the ability of people to communicate, collaborate and express themselves, yielding immense social and economic benefits both within Australia and globally. However, these same communications technologies are also routinely misused to enable, facilitate and carry out criminal activity and to undermine Australia's national security. For example:

- the Secretary-General of the United Nations has observed that '[t]he Internet is a prime example of how terrorists can behave in a truly transnational way',[1] and the United Nations has identified that modern communications technologies underpin terrorist propaganda (including recruitment, radicalisation and incitement to terrorism), financing, training, planning and execution[2]
- serious criminals and organised criminal groups make extensive use of communications technologies to plan and carry out crimes, including to engage with specialist money launderers and other criminal facilitators
- child exploitation rings hide their activities by setting up secure file-sharing networks from inside the comfort of their homes, and
- corrupt public officials use the full suite of communications technologies to abuse their positions of trust.

In recognition of these issues, Parliament has granted a limited number of Australian law enforcement and national security agencies powers to access the content of communications and non-content telecommunications data under the TIA Act. These powers have long been amongst the most effective investigative tools available to agencies to investigate and combat serious and organised crime, corruption, and threats to national security.

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:[3]

> *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 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.

---

[1] Ban Ki-Moon, quoted in United Nations Office on Drugs and Crime (2009) *The use of the Internet for terrorist purposes*, iii.
[2] Ibid, 3.
[3] UNODC, *Current practices in electronic surveillance in the investigation of serious organized crime* (2009) 1.

The power to lawfully access 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.

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

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. 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 begin their investigations several steps behind perpetrators. Agencies use telecommunications data and lawfully accessed communications 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 agent 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 physical surveillance, cannot provide essential historical information required in criminal investigations.

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 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 its nature, has a limited physical footprint. For online investigations, telecommunications data and content is, in many cases, the principal 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. 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. Instances of espionage and foreign interference within Australia have continued to increase, both in terms of the number of occurrences and the range of operatives. In particular, the scale and sophistication of cyber-espionage conducted against

Australian Government and private sector systems has increased significantly in recent years.[4] 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.[5] As the persons involved undertake this activity in 'cyberspace', access to telecommunications data and the lawful interception of their communications are often both crucial aspects of counter-espionage investigations.[6]

Telecommunications data is becoming increasingly important to Australia's law enforcement and national security agencies as they lose reliable access to the content of communications. This threat has increased significantly since the Snowden disclosures. As such, even where agencies cannot obtain the content of the communications, they have historically often been able to use metadata to determine how and with whom a person has been communicating. The ability of agencies to map networks through metadata is an important investigative tool.

Considering the investigative and technological environment in which our agencies now operate, 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 criminal acts and security threats in this country.

Challenges facing Australia's law enforcement and national security agencies

Australia's law enforcement and national security agencies are facing a trio of interrelated challenges:

- a long-term decline in the availability of lawfully accessed telecommunications data
- a long-term increase in the importance of access to telecommunications data, which has accelerated in the past 18 months, and
- an increasingly high-risk operational environment, driven by but not limited to an increased risk of terrorist attacks in Australia.

[4] ASIO Report to Parliament 2013-14, 6.
[5] Ibid.
[6] Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper (2012) 15.

Diminished capability to lawfully access communications—the 'going dark' problem

Agencies' ability to reliably obtain the content of communications under a warrant issued under the TIA Act is diminishing. This decline in capability has been a long term trend, driven by technological change and the globalisation of telecommunications. This trend has previously been labelled the 'going dark' problem, as it seriously degrades the ability of law enforcement and national security agencies to obtain intelligence and evidentiary material from inside organised criminal groups and terrorist cells. One of the implications of this challenge is that agencies are increasingly reliant on alternative investigative techniques, including access to telecommunications data.

Diminished capability to lawfully access telecommunications data

Despite the critical nature of telecommunications data to investigations, Australia's telecommunications industry has some obligations to retain this information but these obligations are not sufficient for law enforcement and security purposes. This is inconsistent with the approach taken in a number of other industries, where the keeping of certain records is critical to law enforcement and/or national security, including the banking and finance, remittance and gambling industries,[7] the airline industry,[8] and all taxpayers.[9]

Rapid changes in communications technology, and in the business practices of Australian telecommunications companies, are resulting in companies keeping fewer types of telecommunications data that are critical to law enforcement investigations, and keeping those records for shorter periods of time. As this Committee identified in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, this change 'has resulted in an actual degradation in the investigative capabilities of the national security agencies, which is likely to accelerate in the future.'[10] That trend has continued unabated since the Committee's report, with further, significant reductions in the period for which certain service providers retain critical telecommunications data.[11]

It is important to distinguish between industry retaining telecommunications data in general, and retaining the types of telecommunications data that are critical to law enforcement and national security investigations. While it is true that, across the telecommunications industry, more telecommunications data is generated and retained than at any previous point in history, much of this data is of limited, if any, investigative value and would not be subject to data retention obligations.

Telecommunications data is used in almost all national security investigations conducted by the Australian Security Intelligence Organisation (ASIO), including almost all counter-terrorism, espionage and intelligence investigations, and all cyber-security investigations. Telecommunications data is also used in almost all serious law enforcement investigations, including almost all counter-terrorism, cyber-crime, organised crime, drug trafficking, anti-corruption and serious criminal (such as murder, serious sexual assault or kidnapping) investigations.

More generally, telecommunications data is critical to the investigation of almost any criminal activity, serious or otherwise, and almost any activity prejudicial to security that has been facilitated, enabled

---

[7] *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, Ch 8.
[8] *Customs Act 1901*, s 64ACA, noting that passenger records must be provided to Customs, rather than being kept by each airline.
[9] *Income Tax Assessment Act 1936*, s 262A.
[10] [5.207].
[11] See, for example, Parliament of Australia, *Parliamentary Debates*, House of Representatives, 30 October 2014, 12561 (Malcolm Turnbull, Minister for Communications).

or carried out via communications technology. Electronic communications, by definition, do not leave a physical footprint, allowing individuals and groups to plan and carry out such activities without risk of detection via many 'traditional' investigative techniques. As such, the records kept by telecommunications companies about the services they have provided (telecommunications data) are often the only source of information available to agencies to identify and investigate individuals and groups using communications technologies for such purposes.

In particular, reliable access to telecommunications data is essential for cybercrime investigations, criminal and national security investigations involving online communications, and investigations involving the production and sharing of child exploitation material online. Agencies use a range of investigative techniques to investigate and combat such crimes, however without reliable access to records of which Internet Protocol (IP) address was allocated to a particular subscriber at a point in time, agencies are generally unable to attribute criminal activity back to a real-world person.

For example, in a current child exploitation investigation, the AFP has been unable to identify the users behind 156 out of 463 IP addresses linked to apparent criminal activity, because certain Australian internet service providers do not retain the necessary IP address allocation records.

In 2011, the Bundeskriminalamt (BkA or German Federal Police) completed a statistical analysis of their access to telecommunications data, following the annulment of Germany's data retention laws.[12] That analysis concluded that, of the investigations in which telecommunications data was accessed, that telecommunications data provided the *only* investigative lead in 45.4% of cases. Telecommunications data made an 'important' contribution to the investigation in 92.7% of the remaining cases.[13]

Data is used throughout investigations, but is particularly used during the early stages of investigations to:

- identify suspects, associates and criminal networks
- rapidly rule out innocent parties from further investigation
- identify patterns of illegal behaviour, and
- provide the basis to apply for warrants for the use of additional powers, such as search or interception powers.

Almost all investigations require agencies to use one or more investigative techniques to undertake the above steps. For example, in all investigations, agencies must identify suspects. Similarly, it is always desirable to rule innocent parties out from suspicion as early as possible, both to prevent any unnecessary intrusion on their privacy, and to ensure that scarce investigative resources are used efficiently. While all investigative techniques involve some degree of intrusion, the use of telecommunications data is one of the least privacy intrusive investigative tools available to agencies.

Accordingly, where telecommunications data is not retained, it often prevents investigations from progressing. For example, in June 2014 the AFP received information from Interpol about a suspect who had made a statement online that they intended to sexually assault a baby. Interpol provided IP

[12] Bundeskriminalamt, *Stand der statistischen Datenerhebung im BKA [Statistical analysis of data collection in the BkA]*, 13.
[13] Ibid.

address details belonging to an Australian carrier. As the Australian carrier only retained data for a maximum of 7 days, no results were available and the suspect was unable to be identified.

In the best case, agencies may be able to progress investigations by using more resource-intensive investigative methods (limiting their capacity to investigate other matters) or more intrusive investigative techniques.

In the worst cases, a crime or threat to security will not be adequately investigated.

Increased threat environment

The above challenges apply across all significant national security, law enforcement and anti-corruption investigations. However, these challenges are being significantly exacerbated by the current increased counter-terrorism threat environment, increasing the urgency of the need for a response.

Australia faces an increased risk of terrorist attacks, linked to the increasing number of Australians working with, connected to, or inspired by a range of terrorist groups, including the Islamic State, Jabhat al-Nusrah, and Al-Qa'ida. While the risk of terrorism in Australia is not limited to any one religion or conflict, the Australian Government is particularly concerned that individuals in Australia will be inspired by the conflict in Syria and Iraq to promote, incite and commit terrorism here. Returned foreign fighters from these conflicts have already planned and carried out attacks in Europe, and Australian authorities disrupted and prevented a number of terrorist attacks in Australia planned by individuals who returned from fighting or training in Afghanistan in the early 2000s.

ASIO, AFP and other law enforcement agencies have experienced a significant rise in the volume and complexity of their counter-terrorism investigations in the past 18 months.[14] Agencies appropriately prioritise their resources to respond to increased threats. However, in an increased threat environment characterised by a higher operational tempo, there is a narrower margin for error in law enforcement and national security investigations. This narrower margin is particularly evident in relation to 'lone wolf' threats: such persons have limited, if any, contact with other known extremists, giving authorities fewer opportunities to detect their activities and intentions. As such, any missed opportunity to identify and prevent these attacks represents a significant risk.

In this environment, the existing capability gaps outlined above represent an urgent and increasing threat to not only public safety and national security, but also to the ability of Commonwealth, State and Territory governments to continue effectively enforcing Australia's criminal laws.

Alternatives to mandatory data retention

Introducing a voluntary code of practice for data retention

One alternative to a mandatory data retention scheme would be to develop a voluntary industry code of practice for data retention. Industry codes of practice are made under the *Telecommunications Act 1997* and are approved by the Australian Communications and Media Authority. There is some precedent for imposing data retention obligations under voluntary codes of practice in Australia. For example, under the *Telecommunications Consumer Protection Code 2012* (TCP Code), the

[14] Australian Security Intelligence Organisation, *ASIO Report to Parliament 2013-14*, 29; Australian Federal Police, *Annual Report 2013-14*, 34.

telecommunications industry has agreed that carriage service providers should retain billing information for six years for consumer protection purposes.

The Department does not consider that a voluntary industry code would be an effective solution to the current challenges. The existing data retention obligations under the TCP Code apply inconsistently between service providers, and between individual services offered by the same provider. 'Billing information' is limited to information required to bill a subscriber. For 'traditional' telephony services that are billed on a per-call basis, the TCP Code requires providers to keep many types of telecommunications data that are critical to law enforcement and security investigations, including call charge records. However, these obligations do not apply in relation to many new and emerging services, such as untarrifed, unlimited or 'infinite' plans that are commonly offered by providers of Voice over IP (VoIP) services, and that are increasingly being released by fixed-line and mobile service providers. Media reporting suggests that Australia's mobile providers are currently migrating to entirely IP-based networks that would largely remove the need for per-call billing, creating a substantial risk that the proportion of services covered by the obligation under the TCP Code to retain billing records will decline dramatically in the next 24 months.

More broadly, the Australian Government has, over a number of years, attempted to engage with service providers to ensure that service providers understand the critical importance of telecommunications data to law enforcement and national security investigations and to provide agencies with advance warning of any significant changes to their commercial data retention practice to allow agencies to take steps to mitigate impacts on ongoing investigations. While many service providers appreciate the importance of reliable access to telecommunications data to law enforcement and national security investigations, this appreciation has not prevented carriers from making commercial decisions that have substantially degraded agencies' investigative capabilities. For example:

- In mid-2013, a major Australian ISP reduced the period of time for which it retains IP address allocation records from many years to three months. IP address allocation records are information about the number allocated to a service to allow it to communicate on the internet, much as a phone number allows a phone service to make calls on a network. The ISP had previously agreed to provide the Australian Government with advanced notice of any significant change in its retention practices, to allow agencies to mitigate the impact on ongoing investigations, but failed to do so. As a result, a number of Commonwealth, state and territory law enforcement and national security investigations were impacted. In the previous 12 months, ASIO had requested IP address allocation records covering periods outside the new 90-day retention window as part of counter-terrorism and counter-espionage investigations. Were these investigations to take place today, critical information would not be available.
- In late 2013, a major Australian carrier deleted its holdings of a critical type of telecommunications data as part of a system upgrade. As a direct result of this action, agencies are unable to reliably identify suspects or execute interception warrants on this carrier's network.

The international experience is that service providers are unlikely to consistently and uniformly comply with a voluntary scheme. For example, UK service providers refused to comply with the UK voluntary code of practice,[15] introduced in December 2003.[16]

[15] *Retention of Communications Data (Code of Practice) Order 2003* (UK).

Expanding the existing preservation notice regime

A second alternative to mandatory data retention that has been suggested by a number of commentators and members of Parliament is to expand the existing preservation notice regime to apply to telecommunications data. The rationale for this approach is that, once an agency has identified a suspect, it would be able to request that service providers preserve associated telecommunications data for later access.

The preservation notice regime was introduced into the TIA Act by the *Cybercrime Legislation Amendment Act 2012*, to facilitate Australia's accession to the Council of Europe's *Convention on Cybercrime*. Preservation notices are made under Part 3-1A of the TIA Act, entitled 'Preserving stored communications', and require carriers to preserve 'stored communications', such as emails and voicemail messages when served with a notice. Preservation notices may extend to the telecommunications data associated with such messages (such as requiring the service provider to preserve information about the time and date at which a voicemail message was left, as well as the actual message), but cannot be used to require providers to preserve other telecommunications data, such as data relating to telephone or VoIP calls, or IP address allocation records. As such, the existing regime would need to be expanded to enable preservation of telecommunications data.

However, the Department's view, supported by international experience, is that expanding the existing preservation notice regime would not address the capability challenges faced by agencies. Preservation and data retention are complementary tools, but are aimed at different objectives. The purpose of preservation notices is to 'quick freeze' volatile or perishable electronic evidence that a provider possesses for a short period of time, to allow agencies time to apply for and obtain a warrant to access that information. Evidence cannot be preserved if it was never retained, or if it has already been deleted. For example, a preservation notice issued 9 months after a criminal event cannot assist an investigation if the data sought was destroyed after just 1 month's existence.

Preservation notices will not, therefore, address the fact that service providers are not retaining critical types of telecommunications data, or are retaining that data for shorter periods of time. In addition, as the current data authorisation provisions in Chapter 4 of the TIA Act already facilitate timely access to telecommunications data for legitimate investigative purposes, the Australian Government did not need to include preservation notices for telecommunications data in the Cybercrime Act.

By comparison, the purpose of data retention is to introduce a consistent record-keeping requirement across industry to ensure that certain telecommunications data are consistently available. As such, data retention is in fact a prerequisite to preservation of data, rather than preservation offering an alternative to retention.

The Department's view on this matter is consistent with the views of the Council of Europe,[17] the European Commission,[18] and the Netherlands Government,[19] each of which has reviewed whether

---

[16] All Party Parliamentary Internet Group, Parliament of the United Kingdom, *Communications Data: Report of an Inquiry by the All Party Internet Group* (2003) [139].
[17] Cybercrime Convention Committee, Council of Europe, *Assessment Report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime* (2012), 75-6.
[18] Centre for Strategy and Evaluation Services, *Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries* (2012), 22-3 (Report prepared for the Directorate General for Home Affairs, European Commission).
[19] Ministry of Security and Justice, Netherlands Government, *The Dutch implementation of the Data Retention Directive* (2013) 110-11.

preservation is a viable alternative to data retention. Each of those bodies has found that a 'quick freeze' preservation scheme cannot substitute for data retention.

Warrants for telecommunications data

Some commentators have asserted that, on grounds of privacy, it would be more appropriate for there to be independent oversight of agencies' access to telecommunications data, such as by requiring agencies to obtain a warrant from a judicial officer or a member of the Administrative Appeals Tribunal before it may access telecommunications data.

While it is important that there are strong safeguards around the use of intrusive powers, these safeguards must be carefully designed to ensure that they do not impede agencies effectively performing their functions.

The Bill does not introduce a requirement for agencies to obtain a warrant to access telecommunications data. The benefits of introducing a warrant regime would be outweighed by the impact on agencies' ability to combat serious crime and protect public safety.

Timely access to telecommunications data can provide agencies with vital leads before evidence can be lost or destroyed. However, warrant applications are resource intensive, and can take days, if not weeks, to prepare and complete. Delaying an agency's ability to begin an investigation by this length of time would seriously harm their ability to investigate crimes or threats to national security.

Telecommunications data is used most commonly in the early stages of an investigation, when evidence is at risk of being lost, or where victims might be in imminent risk of danger. For example, a police force investigating a suspected kidnapping would often begin their investigation by seeking information about whom the victim had been communicating with immediately prior to their kidnapping. Early information about the whereabouts of the victim would increase the chances of a successful rescue.

Warrants are also typically reserved for the most intrusive powers, such as the power to enter a home, intercept phone calls, or access stored communications. Many information-gathering powers that are exercised by agencies under Commonwealth, State and Territory laws do not rise to that level of intrusiveness and may be exercised without a warrant. Examples of such powers are powers to obtain banking, financial and healthcare records. The power to access data is only of the same level of intrusiveness as these powers. Non-warranted access to information is a normal part of any law enforcement framework.

Furthermore, to require a warrant in this circumstance would be counterintuitive to the fundamental tenet of proportionality because telecommunications data serves to establish the case for more intrusive powers to be deployed under a warrant.

In relation to suggestions that a 'generic' warrant be created for access to telecommunications data, the Department notes that in some European jurisdictions investigating judges and public prosecutors are able to authorise the disclosure of data for the purposes of whole investigations, rather than on a disclosure-by-disclosure basis, as is the case under the TIA Act.

However, the UK's Interception of Communications Commissioner notes in relation to such data access regimes that exist in Europe:

> *These general orders might satisfy the basic necessity test, but we would question how proportionality can be judged properly under such a system. The exception to this practice appears to be limited to the*

> *United Kingdom, Ireland and France – those Member States have laws that require each acquisition of data to be considered and authorised individually*.[20]

The Australian scheme is comparable to that which exists in the UK where a disclosure of information to be sought individually which allows the proportionality of each particular disclosure to be considered separately. This is required by section 180F of the TIA Act, which provides that authorising officers must have regard to whether any interference in the privacy of any person or persons that may result from a particular disclosure is justifiable, having regard to the likely relevance and usefulness of the information and the reason why the disclosure or use is proposed to be authorised.

Those considerations are important checks that would possibly be lost from the investigative process if 'generic' whole-of-investigation warrants were to be adopted. The checks may be lost as the issuing authority would be required to decide whether or not to authorise disclosure of information without knowing the relevance of particular pieces of information to an investigation or the privacy impact of any such disclosures.

The Department's view is that the current law and policy settings in the TIA Act are preferable, as they require the person authorising the disclosure of this basic investigative material to turn their mind to privacy and proportionality considerations when deciding whether or not to authorise particular disclosures.

Get a Warrant Bill

A proposal to require agencies to obtain a warrant has been previously canvassed in the Telecommunications Amendment (Get a Warrant) Bill 2013 (the Get a Warrant Bill).

The Attorney-General's Department made a submission to the Senate Standing Committee on Legal and Constitutional Affairs' 2013 inquiry on the Get a Warrant Bill. The submission discussed the disproportionate impact on the operational capabilities of law enforcement and national security agencies.

In particular, AGD's submission noted that:

- enforcement agencies would be hampered in their investigations, particularly in the time critical initial stages of investigations
- agencies that need to apply for interception or stored communications warrants would be heavily constrained in their ability to obtain the preliminary information required to support their warrant application for the most capable investigative tools (a 'catch 22').
- alternative investigative powers, such as physical surveillance and search powers, would be more privacy intrusive than accessing telecommunications data.
- agencies as well as issuing authorities would be unable to cope with the large number of new warrant applications that would be required, and
- Australia may be placed in breach of its obligations under the Cybercrime Convention.

The Department's submission to the Get a Warrant Bill inquiry is included at **Appendix C**.

---

[20] Interception of Communications Commissioner's Office, United Kingdom Government, *Evidence for the Investigative Powers Review* (2014) 32.

Independent oversight instead of warrants

Independent oversight of an agency's access to data is preferable to requiring that agencies obtain warrants.

The Bill introduces independent oversight by the Commonwealth Ombudsman of law enforcement agencies that access and use telecommunications data (see also new Ombudsman amendments at page 50).

Independent oversight has a very similar psychological effect to a warrant process. Knowing that an agency's access to data is going to be scrutinised by an independent overseer is a strong deterrent against non-compliance or misconduct. Further, an oversight body can review how an agency has accessed and used the information from end-to-end, while a warrant issuing authority only sees the initial application. Most importantly, independent oversight by the Ombudsman will not delay agencies during the early hours of an investigation.

In the past, the Ombudsman has found in assessing stored communications access provisions that there was an overall high level of agency compliance, and agencies have positively addressed the Ombudsman's recommendations by updating relevant policies and procedures to help staff to comply with the TIA Act.

Warrant requirement in the United Kingdom

The UK has introduced a partial warrant-for-data scheme which has proved counter-productive to the objective of investigating and punishing criminal conduct. In the UK, the *Regulation of Investigatory Powers Act 2000* (RIPA) governs access to telecommunications data (described as communications data in the RIPA). Section 22(4) of the RIPA provides that a designated person may issue a notice requiring a telecommunications provider to disclose communications data. Section 22(2) of the RIPA lists a range of purposes for which communications data can be obtained, such as for national security or law enforcement.

In 2012 the United Kingdom implemented the *Protection of Freedoms Act 2012 (Judicial Approvals for Local Authority Communications Data Requests)*, which introduced a warrant regime for local authorities to access telecommunications data. Affected agencies faced delays of up to six weeks to obtain warrants, and reduced the number of applications by more than two-thirds.

The UK Interception of Communications Commissioner has responsibility for oversighting the UK interception regime. In his 2012 *Annual Report of the Interception of Communications Commissioner*, the Rt Hon Sir Paul Kennedy discussed the new warrant requirements for accessing telecommunications data (at pages 63-64). The Commissioner stated that the decrease in applications was likely 'due to the overly bureaucratic and costly process now in place'. The Commissioner said that a warrant requirement would not 'have any impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data'. The Commissioner also recommended that the warrant regime be repealed because 'there is a serious danger that the types of crime that cause real harm to the public… will not be investigated due to the difficulties with the judicial approval process.'

The February 2013 the UK's Intelligence and Security Committee (ISC) issued its report *Access to communications data by the intelligence and security agencies*. The report said (at page 26) that requiring warrants for data could have a significant impact on agency operations and was not justified.

The UK ISC was of the view that retrospective review by the Interception of Communications Commissioner provided sufficient oversight of the process.

The Data Retention Bill and legal professional privilege

Another issue that has been raised is the implications of the Data Retention Bill for legal professional privilege.

At common law, confidential communications between a client and the client's legal adviser are privileged, whether oral or in the form of written or other material, if made for the dominant purpose of submission to the legal adviser for advice (whether connected with litigation or not) or for use in existing or anticipated litigation.

At common law, legal professional privilege attaches to the content of privileged communications, not to the fact of the existence of a communication between a client and their lawyer (See: *National Crime Authority v S* [1991] FCA 234). This distinction is demonstrated in the routine practice of parties to proceedings filing affidavits of documents listing documents in their possession that are not being produced on the ground of privilege, thereby disclosing the fact of the existence of the document.

The uniform evidence laws contain provisions codifying 'client legal privilege' as it applies to evidence led in court, however these provisions do not apply to pre-trial procedures (such as discovery, subpoenas, search warrants or access to telecommunications data as part of an investigation), where the common law continues to apply.

Proposed new paragraph 187A(4)(a) puts beyond doubt that service providers are not required to keep, or cause to be kept, information that is the content or substance of a communication. Section 172 of the TIA Act also provides that an authorisation for the disclosure of telecommunications data made under Chapter 4 of that Act does not permit the disclosure of information that is the contents or substance of a communication, or a document to the extent that the document contains the contents or substance of a communication.

The TIA Act also provides that it is a criminal offence, punishable by two years' imprisonment, for a person to access a stored communication without lawful authority (section 108). The TIA Act also makes it an offence to disclose information obtained by unlawfully accessing a stored communication (section 133). As such, the data retention regime, and agencies' powers to access telecommunications data more broadly, do not affect or authorise the disclosure of the content of any communication, including any privileged communication.

The Data Retention Bill and journalists' sources

A number of commentators have queried the interaction between the Data Retention Bill and journalists' sources, including in some cases suggesting that a special status should be afforded to the telecommunications data of journalists regarding their interactions with public sector whistleblowers.

Disclosures of data are available to support the enforcement of the criminal law, administration of pecuniary penalties and the protection of the public revenue. It is not appropriate to afford a special status to particular types of communications as powers of this type should, by their nature, be applied generally. However, to the extent that concerns relate to the disclosure of the identity of legitimate whistle-blowers, it is important to note that such persons have specific protection under the *Public Interest Disclosures Act 2013* (PID Act). The effect of those protections is that disclosures by

legitimate whistle-blowers are not criminal acts. Accordingly, telecommunications data would not be available by reason of the disclosure.

The PID establishes a legislative scheme to investigate allegations of wrongdoing in the Commonwealth public sector and provide robust protections for current or former public officials who make qualifying public interest disclosures under the scheme. The scheme applies to the officials of law enforcement agencies and, in a more limited fashion, to the intelligence community.

The PID Act protects Commonwealth officials from liability for making a 'public interest disclosure'. The scope of a 'public interest disclosure' is broad, and includes disclosures in relation to criminal conduct, maladministration, abuses of the public trust and abuse of the office of a public official.

Access to journalists' telecommunications data in the UK

On 9 December 2014, the UK Home Office published a draft Code of Practice discussion paper on access to data. This issue of access to journalists' telecommunication during the investigation of crimes had been raised as an issue by that profession. The draft code of practice makes clear that communications data is not subject to any form of professional privilege. However, the Code notes that access to data relating to some professions may have a higher degree of privacy interference (the draft code specifies doctors, lawyers, journalists, MPs and ministers of religion).

Some media reports had suggested that the UK Government was considering requiring law enforcement agencies to obtain warrants to access journalists' data. Rather than warrants, the Home Office proposes that authorising officers should give special consideration to necessity and proportionality when considering authorising the disclosure of data relating to the particular professions noted above.[21]

In the Australian context, the Department notes that legitimate whistleblowers are immune from all criminal, civil and administrative liability under the PID Act. As such, data access powers will generally not be available to law enforcement agencies in relation to genuine whistleblowers by reason of those disclosures alone.

Operation of Schedule 1 of the Bill

Schedule 1 contains the amendments to require telecommunications service providers to retain certain telecommunications data for a period of two years. The amendments contained in Schedule 1 will also provide for:

- data retention implementation plans
- exemptions from the data retention requirements
- enforcement of data retention obligations
- a review of the operation of the data retention scheme by the PJCIS, and
- annual reporting on the operation of the data retention scheme.

[21] Home Office, United Kingdom Government, *Acquisition and Disclosure of Communications Data – Code of Practice* (2014) 32.

Application of data retention obligations

Proposed new section 187A will apply data retention obligations to communications services provided by Australian carriers, carriage service providers and internet service providers, subject to a number of substantial exceptions and an exemptions regime. The exceptions and exemptions regime will ensure that data retention obligations are tailored having regard to law enforcement and security imperatives as well as compliance cost and related industry considerations.

First, data retention obligations will not apply to services provided to a person's 'immediate circle',[22] such as internet and intranet services provided within corporate and university networks. This exception reflects an assessment that the law enforcement and national security benefit of imposing data retention obligations on these networks would be outweighed by the privacy and compliance burden. While corporate crime and foreign commercial espionage, in particular, are of significant concern, agencies typically enjoy a high level of cooperation from enterprises responsible for those corporate networks.

Second, data retention obligations will not apply to services that are provided only to a single place, or to places in the same area, such as free Wi-Fi access provided in restaurants, libraries or a campus.[23] This exception reflects an assessment that the law enforcement and national security benefit of imposing data retention obligations on these services would be outweighed by the privacy and compliance burden.

However, some key non-content data relating to the communications made from internet cafes will be retained by the internet service providers, supplying those services to the internet cafes. This will assist with any authorisation requests issued by agencies seeking to advance their investigations.

The Communications Access Co-ordinator (CAC)[24] may declare that data retention obligations apply to particular services that would otherwise be exempt under proposed new subsection 187B(1). When making such a declaration, the CAC must have regard to the interests of law enforcement and national security, the objects of the Telecommunications Act,[25] and any other matter the CAC considers relevant. The declaration-making provides the flexibility to apply data retention obligations to services or networks operated by particular companies (such as companies operating critical infrastructure), or in particular buildings or places, where this is consistent with the requirements of law enforcement or national security.

Third, data retention obligations do not apply to broadcasting services, such as radio or television networks.

---

[22] Subparagraph 187B(1)(a)(i).
[23] Subparagraph 187B(1)(a)(ii).
[24] The Communications Access Co-Ordinator is a statutory office that is held by Secretary of the Attorney-General's Department or another person specified by the Attorney-General in a legislative instrument, and which is currently held by the First Assistant Secretary, National Security Law and Policy Division of the Department.
[25] The main (but not the only) objects of the Telecommunications Act are set out in section 3(1) of that Act and are to provide a regulatory framework that promotes the long-term interests of end-users of carriage services or of services provided by means of carriage services, the efficiency and international competitiveness of the Australian telecommunications industry, and the availability of accessible and affordable carriage services that enhance the welfare of Australians.

Fourth, proposed new section 187K will allow the CAC to exempt or vary data retention obligations for specified service providers (including specified classes of service providers), either on application or of his or her own motion. When considering whether to grant an exemption, the CAC must consider a detailed set of matters, including the interests of law enforcement and national security and the objects of the Telecommunications Act, as well as the provider's compliance history, the costs or anticipated costs of complying with full data retention obligations, and any alternative data retention arrangements that the provider has identified. The Department notes that, due to the considerable variability between services offered by different providers, exemption applications will generally be considered on a case-by-case basis. However, the Implementation Working Group has identified a range of services that may be possible candidates for exemption, including:

- IPTV
- On-demand video service
- Internet Radio
- Music Streaming
- Dark Fibre
- Telehealth services
- Lifelogging services

Application to 'offshore' service providers

Data retention obligations will apply to service providers that are within Australia's territorial jurisdiction. That is, obligations will apply to providers that own or operate infrastructure, such as servers, routers and/or cables, within Australia that enables one or more of their communications services. The obligations are framed in this way to ensure that service providers cannot avoid their data retention obligations by off-shoring part of their infrastructure or outsourcing the provision of some services to overseas entities.

The Department acknowledges that there are a number of service providers that have a significant presence in the Australian telecommunications market that do not own or operate such infrastructure in Australia, and that therefore will not be covered by data retention obligations, including the major social media providers. However, many companies based in foreign jurisdictions are subject to data retention laws in those jurisdictions, reducing the need for Australian legislation. Additionally, as a party to the Cybercrime Convention, Australian law enforcement agencies are able to obtain expedited assistance from 43 countries to obtain telecommunications data held in those countries that is relevant to Australian investigations.

More broadly, attempting to impose extraterritorial data retention obligations would give rise to significant jurisdictional and conflict-of-laws issues including where, for example:

- providers are already subject to data retention laws in their own jurisdiction, leading to the provider being subject to inconsistent Australian and foreign obligations, and
- providers are subject to data minimisation obligations in their own jurisdiction, leading to the provider being subject to contradictory obligations to retain and delete telecommunications data.

Data retention obligations—the dataset

Proposed new section 187A will establish a minimum obligation on telecommunications service providers to keep a limited set of telecommunications data. The details of the draft data set are contained in the 'Proposed Data Set' document referred to this Committee and published on the

Department's website on 31 October 2014. A legislated data retention scheme will create an industry-wide common standard for data retention practices.

Privacy and proportionality considerations have been central to the development of the proposed categories of data that the data retention obligations will apply to. The data retention obligations have been strictly limited to data that is vital to law enforcement and national security investigations, and was developed based on advice from law enforcement and national security agencies and feedback from the telecommunications industry.

The dataset is based closely on the former European Union Data Retention Directive. **Appendix A** provides a table comparing these categories with the Directive. However, the proposed data set draws on international experience[26] to ensure the proposed Australian obligation is able to adapt to the continuous evolution of communications technology. The Government has adopted two key measures to future-proof the data retention regime.

First, the proposed Australian dataset has been drafted to be more technologically neutral than the Directive, to prevent it from rapidly becoming obsolete as a result of ongoing technological change. This approach is also consistent with the views of the Australian Law Reform Commission, that a technology neutral approach to defining telecommunications data should be maintained, to ensure that the TIA Act can be applied to new developments in technology.[27] This more technology-neutral approach will require Government to provide industry with a greater degree of guidance about how data retention obligations should be implemented at a technical level. Accordingly, the Government has established the Implementation Working Group (IWG), a joint industry-Government working group tasked with, among other things, refining the data retention data set and supporting implementation of data retention obligations.

Second, the Bill provides for a regulation-making power to prescribe the data that is to be retained. This regulation-making power is expressly limited to six categories of telecommunications data set out in proposed new subsection 187A(2), being information about the:

- subscriber or account holder of the telecommunications service
- source of a communication
- destination of a communication
- time and duration of a communication
- type of communication, and
- location of equipment used in the communication.

The data retention obligation is also subject to a range of additional exclusions and limits set out in proposed new subsections 187A(4) and (7), which are discussed further below.

A regulation-making power for the data set is included to provide sufficient details about the data retention obligation to afford industry certainty and to provide appropriate transparency and detail to users of telecommunications services. This level is greater than that typically included in primary legislation.

---

[26] Centre for Strategy and Evaluation Services, *Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries* (2012), 25 (Report prepared for the Directorate General for Home Affairs, European Commission); Ministry for Security and Justice, Netherlands Government, *The Dutch implementation of the Data Retention Directive* (2013) 136.
[27] *For your information: Australian privacy law and practice* (2008) [73.33].

Using regulations to provide for the data set will also ensure that the data retention regime is able to be updated in response to changes to communications technologies, business practices, and law enforcement and national security threat environments. The telecommunications industry is highly innovative and increasingly converged. Sophisticated criminals and persons engaged in activities prejudicial to security are frequently early adopters of communications technologies that they perceive will assist them to evade lawful investigations.

Substance of the data set

Data retention obligations will apply to a limited subset of telecommunications data generated and retained by the telecommunications industry. The Department provided a document outlining a working definition of telecommunications data during the previous 2012 PJCIS inquiry. This document explained that telecommunications data is information that allows a communication to occur (also known as 'traffic data') and information about the parties to a communication (also known as 'subscriber data'). The document then provided a number of specific examples of each type of information. Data retention obligations, by comparison, will apply only to a limited subset of telecommunications data, as set out in the proposed dataset.

The proposed data set is based on current, best-practice retention practices within the telecommunications industry and does not require the retention of telecommunications data that is not currently retained by at least one provider. However, different providers may need to modify aspects of their current retention practices to meet the proposed new industry standard.

Consistent with the PJCIS's 2013 recommendation that 'any mandatory data retention regime should apply only to meta-data and exclude content', proposed new paragraph 187A(4)(a) expressly provides, for the avoidance of doubt, that the data retention obligation does not require service providers to retain the contents or substance of a communication. Similarly, consistent with the PJCIS' 2013 recommendation that 'internet browsing data should be explicitly excluded' proposed new paragraph 187A(4)(b) expressly provides that service providers are not required to retain an address to which a communication was sent on the internet that the provider only has as a result of providing an internet access service – the effect of which is to provide that a service provider is not required to keep web-browsing history.

The Parliamentary Joint Committee on Human Rights (PJCHR) has recommended that, to ensure that the content of communications is not retained the Bill should exhaustively define what constitutes 'content'. The Scrutiny of Bills Committee has also recommended that consideration be given to this issue. The Department's view is that while it is important to ensure that data retention obligations do not apply to the content or substance of communications, the PJCHR's recommendation would actually have the contrary effect as an exhaustive definition would not keep pace with technological change, leading to an increasingly wide range of information that may not be excluded from data retention obligations. The technologically-neutral approach taken to defining the content or substance of a communication under the TIA Act is consistent with the approach taken by the *Privacy Act 1988* and Part 13 of the Telecommunications Act, and is consistent with the 2008 views of the ALRC about the desirability of technological neutrality in this field.

Paragraph 187A(2)(a)—subscriber of the relevant service and accounts, telecommunications devices and other relevant services relating to the relevant service: The information listed under item 1(a) of the proposed data set for the purposes of paragraph 187(2)(a) is essential for any investigation involving communications made from a service, as it assists investigating authorities to establish the details of who is involved in making a communication through the identification of the

subscriber to the service. In the absence of the retention of this type of information, it may be exceedingly difficult or impossible to determine who has made a communication of interest. Importantly, from a privacy perspective, item 1(a) is limited to information used by the service provider to identify the subscriber—item 1(a) does not impose a 'real name' policy requiring service providers to positively identify each subscriber.

The information listed under item 1(c) (billing, payment or contact information) serves a similar purpose, and is of particular utility where an account is subscribed under a false identity. Billing and payment information is generally more difficult to falsify, and contact information can often provide agencies with further investigative leads to identify who has made a communication of interest.

The information listed under item 1(d) (identifiers relating to the relevant service) includes information such as the phone number or IP address/port number combination allocated to a particular account, service or device at a particular point in time. This information is necessary to allow particular communications of interest to be attributed to a particular account, service or device. Importantly, from a technical perspective, item 1(d) is limited to identifiers used by the service provider—item 1(d) does not require service providers to generate and retain identifiers that are not natively used by their network or service.

The information listed under items 1(b) (contractual information), (e) (status of the service), and (f) (information about the metrics of the service) is critical for a range of technical purposes. Most importantly, this information is vital to allow agencies to properly provision and resource interception warrants. Telecommunications interception, particularly in relation to IP-based services, is highly complex and resource intensive. Inadequate resourcing and provisioning of interception systems can result in potentially inculpatory or exculpatory intercept material being lost, compromising the evidential chain and the overall investigation. The information listed under these items allows agencies to make an informed, risk-based estimate of how many resources need to be allocated to a particular interception warrant (for example, based on this historic usage of the service or services, whether any of those services are no longer active, and the maximum data allowance for each service).

Paragraph 187A(2)(b)—the source of a communication: This category covers the identifier or combination of identifiers which are used by the service provider to describe the account, service and/or device from which a successful or attempted communication is sent. Examples of such identifiers are telephone numbers, email addresses or account names. The source of a communication is critical for the purpose of the investigation, detection and prosecution of serious crime and security threats, providing clear identification of the origin of communications relevant to investigations.

Paragraph 187A(2)(c)—the destination of a communication: This category covers identifiers of an account to which a communication is sent. Examples of such identifiers are the telephone number dialled, or the identifiers to which a VoIP call is made (which, depending on the services involved, could be a traditional telephone number, an email address, account name and/or an IP address). The retention of telecommunications data regarding the destination of a communication (such as telephone numbers and e-mail addresses) is necessary in order to connect a communication of interest to the particular telecommunications service being used to receive this communication. This information can then assist with determining the subscribers who sent or received relevant communications. If providers of telecommunications services did not retain this telecommunications information, there is a real risk that agencies would not be able to determine with whom a person has been communicating.

This information provides important information on linkages and connections of investigative significance, which are critical to advance inquiries into criminality and security threats.

Item 3(b) of the proposed dataset also requires service providers to retain identifiers where a communication is forwarded, routed or transferred.

Importantly, under proposed new paragraph 187A(4)(b), the retention obligation is explicitly expressed to exclude the retention of destination internet address identifiers, such as destination internet Protocol (IP) addresses or uniform resource locators (URLs) for internet access services. This exception is intended to ensure that providers of internet access services are not required to engage in session logging, which may otherwise fall within the scope of the destination of a communication.

However, the general obligation to retain destination information will continue to apply to other services, such as email, messaging or VoIP services that are analogous to 'traditional' communications services. Providers of those and other services will be required to retain the destination identifiers for communications sent using their services.

Further, proposed paragraph 187A(4)(c) makes clear that service providers are only required to keep records about the services they themselves provide and operate. They are not required to keep records about communications sent or received using third-party communications services running 'over-the-top' of their network or service. This means that an internet access service provider, though not required to retain web-browsing information, would have to retain destination information for webmail services, for example, but only if it provided that webmail service itself. That particular provider would not be required to retain destination information for services its customer used, but it did not provide.

Paragraph 187A(2)(d)—the date, time and duration of a communication: This category covers the time at which a communication occurred and its duration. Using this information, agencies can link the time of a communication with events associated with the communication. This information is also critical to linking a communication to a particular subscriber, as the source of a communication can change over time, requiring the time of the communication in order to accurately identify its originator.

The retention of this data category is reasonable, proportionate and necessary as it constitutes information that can help inculpate or exculpate an individual associated with a communication. It is also valuable in tracing the steps of a missing person who has been using a communications service before or during the time they are missing. An agency's ability to investigate these matters will be significantly limited if providers of telecommunications services do not retain this information. The data covered by this item is also critical because communications may now travel over multiple networks and service providers. As such, information about communications needs to be accurately time-stamped to enable agencies to link information from one provider with information from one or more other providers to develop a complete picture of a particular communication.

Paragraph 187A(2)(e)—the type of communication: This category covers the type of service used, including the type of access network or service or application service. Data which identifies the type of communication is necessary for understanding what telecommunications service has been used to send the communication. Because data formats vary considerably across different types of services, this information is essential to allow agencies to reliably interpret information they receive from a service provider.

Paragraph 187A(2)(f)—the location of the line, equipment or telecommunications device: This category covers information which identifies the location of equipment used in connection with a communication. Information on the location of telecommunications equipment can be highly significant to law enforcement and national security investigations. Location information is often retained in records which form a part of a customer's billing.

Location-based data is valuable for identifying the location of a device at the time of a communication. This information can provide a strong indication about whether a person was at the scene of a crime, and is also frequently used to exclude people from suspicion in the early stages of investigations. This data may also be instructive in determining the location of a person who is reporting an emergency, or help identify the location of a missing person who has used a telecommunications device. Without this information agencies' ability to investigate crimes, emergencies and missing person matters are impeded.

Location records are potentially among the most sensitive elements of the proposed dataset. As such, the nature and volume of location information that service providers will be required to keep has been strictly limited to ensure that service providers are not required to keep continuous records about the location of a device, or anything approaching that level of detail. Proposed new subsection 187A(7) provides that two or more communications that together constitute a single communications session, such as an internet access session, are taken to constitute a single communication. Where two or more communications are taken together to constitute a single communications session (for example, on a mobile internet service), location records are only required to be kept in relation to the combined communications session, not for each packet, network location poll or background update, therefore significantly limiting the requirement to retain location information.

The proposed dataset limits the requirement to retain location information to information about the location of a device at the start and end of a communication. Service providers are not required to keep records of the device's location throughout a communication, or more broadly (for example, when a device is active).

In addition, proposed paragraph 187A(4)(c) makes clear that service providers are only required to keep records about the services they themselves provide and operate. They are not required to keep records about communications sent or received using third-party communications services running 'over-the-top' of their network or service. This limitation is particularly important for smartphones, tablets and other mobile devices, which often have many applications running in the background that, in combination, result in the device communicating on a near-continuous basis. This limitation, in conjunction with the two limitations outlined above, ensures that providers are only required to keep a record of the device's location at the start and end of an internet access session. Industry members have advised the Department that a single access session may last from several hours to over six months, depending on the access technology involved.

Finally, proposed new paragraph 187A(4)(e) has the effect of limiting service providers' retention obligation in relation to location information to location information that is used by the service provider in relation to its service. This means that service providers that do not use location information as part of their service are not required to begin collecting that information, and that service providers that do use some degree of location information (such as mobile network providers, who use information about which cell tower a device was connected to in order to route communications) are only required to keep the location information they use to provide the service. Providers will not be required to

conduct additional processing or triangulation to more precisely determine a device's location, beyond what their network does for the purposes of providing the service.

Retention periods

The Bill and draft data set provide for two distinct retention periods:

- service providers are required to retain 'subscriber' records covered by paragraphs 1(a) and (b) of the draft data set for the life of the account plus two years, and
- service providers are required to retain other subscriber records and telecommunications data listed in the data set for two years after they come into existence.

Retention period for subscriber records

The first retention period applies to a subscriber's name, address, identification information and information about the contract or plan which they have subscribed to. A requirement to retain this information for the life of the account plus two years represents a departure from the PJCIS's previous recommendation that 'data retained under a new regime should be for no more than two years'. However, a longer retention period for these particular types of data is necessary as identifying and contractual information tend to be static—it may be provided once when a person signs up to an account or service, and not altered for many years. As such, it is important that service providers continue to retain this information for the life of the account, and do not delete it two years after it comes into existence. This is because subscriber information across the life of the account is useful to interpret transactional data, and in particular, to support attribution of communication. The Department notes that this information will also generally be covered by the TCP Code, which requires service providers to retain 'billing information' for six years.

Two-year retention period

Law enforcement and security agencies advise that a two year retention period is appropriate to maintain their ability to investigate serious crime and threats to national security. While older telecommunications data can be central to investigating both crimes and security threats, the two year retention period seeks to strike a balance between the value in supporting those matters and the additional intrusion and compliance burden that a longer retention period would entail.

Agencies' advice is consistent with the international experience. In 2011, the European Commission conducted a review of the European Union Data Retention Directive. This review was conducted five years after the Directive came into force. The table below shows the breakdown of requests for telecommunications data made by law enforcement agencies under the Directive by age in countries that implemented a two year retention period over the five year period considered by the review.

Age of telecommunications data requested (months)								
	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24
Percentage of requests	57.81%	19.59%	8.03%	5.03%	2.80%	2.00%	1.51%	3.24%
Cumulative percentage of requests	57.81%	77.40%	85.43%	90.46%	93.25%	95.25%	96.76%	100.00%

Summary of age of telecommunications data requested under the EU Data Retention Directive in countries with two-year data retention periods, 2008-12

It is essential to distinguish between the frequency with which agencies access older data, and the importance of that data to investigations when it is accessed: where agencies require access to telecommunications data, its value does not decrease with age. While the review found that approximately 90% of requests for access relate to telecommunications data less than twelve months old, this number is skewed heavily by the use of telecommunications data in more straight-forward 'volume crime' investigations that, despite being serious in nature, can frequently be resolved in a shorter period of time. As such, the above summary obscures the fact that certain types of law enforcement investigations frequently involve longer investigatory periods and therefore require a disproportionate level of access to older telecommunications data. These types of investigations include, but are not limited to:

- counter-terrorism and organised crime investigations, which are often characterised by long periods of preparation. These investigations often require time to establish a clear pattern of relationships between multiple events to expose not just individual suspects, but entire criminal networks, especially where suspects are practicing sophisticated counter-surveillance techniques
- series of related crimes, where agencies are required to piece together evidence from a wide range of sources, not all of which may be immediately evident
- cyber-crimes and other crimes where access to IP-based telecommunications data is required, due to the greater complexity of these investigations—the EU statistics show agencies are up to 7 times more likely to access IP-based data that is more than 12 months old than mobile telephony data
- trafficking in human beings and drug trafficking, where there is often a complex division of labour between accomplices
- serious corruption of public officials, financial crime and tax fraud, where offences are often only detected following audits, or are only reported to law enforcement agencies following internal investigations, requiring agencies to often access data that is already considerably dated
- repeated extortion, where victims are in a relationship with the offender and often only seek help months or even years after the exploitation commenced
- serious sexual offences, where victims may not report the offence for a considerable period of time after the event—for example, the United Kingdom Government has provided advice that over half of the telecommunications data used by its agencies in the investigation of serious sexual offences is more than six months old
- serious criminal offences, particularly in relation to murder investigations, where extensive historical evidence must be assembled to prove intent or premeditation, and
- transnational investigations, which involve significant challenges for agencies attempting to coordinate investigations across multiple jurisdictions, frequently resulting in delays while preliminary information is obtained from foreign agencies.

More broadly, many crimes are not brought to the attention of the relevant authorities until well after the fact, and the normal variability in criminal investigations means that some investigations will continue for considerably longer than average. In such cases, reliable access to telecommunications data can be particularly important, as physical and forensic evidence will frequently degrade with the passage of time.

Commonwealth law enforcement agencies have advised that their usage of telecommunications data closely matches the above profile.

National security investigations, including counter-terrorism and counter-espionage investigations, tend to involve significantly longer timeframes. The nature of clandestine or deceptive activity by foreign states against Australian interests, particularly by sophisticated adversaries, shares some characteristics with complex organised crime and counter-terrorism investigations. Foreign states take a long-term, strategic approach to conducting espionage. The approach is slow and considered in order to hide activities. There is often no known or specific incident or starting point with espionage investigations. ASIO must baseline the activities and threat posed by adversaries over an extended period to identify indicators of activity and then review historical data to understand the extent and scope of the activity and harm.

Differentiated retention periods

Some stakeholders have raised the possibility of having distinct retention periods for the different types of data (for example, internet protocol records versus telephony records). However, as the elements of the proposed data set are interlinked this would significantly impact the utility of data retention as a whole to law enforcement and national security agencies, and would risk compromising its evidentiary value.

For example, a provider keeping call-charge records showing that one phone number has dialled another phone number is significantly less useful to agencies if the provider has not kept associated records showing the time and date on which the phone call occurred.

A number of countries have adopted differentiated retention periods for telecommunications data relating to 'traditional' telephony services and 'modern' IP-based services. In the Department's view, there is no rational basis for such a distinction in relation to the proposed data set. For internet access services, the types of telecommunications data that service providers would be required to retain (subscriber records and IP address allocation records) are less privacy sensitive than the records they would be required to retain for 'traditional' telephony services (including call-charge and limited location records). For 'over-the-top' communications services, such as email and VoIP services, which are broadly similar in functionality and privacy-sensitivity to telephony services, the types of telecommunications data that service providers would be required to retain are analogous to the types of data required for telephony services. The Department's view aligns with the Netherlands Government's review of its data retention laws which concluded:[28]

> *Given that the volume of internet traffic will increase while telephone traffic is likely to decrease further in the future; and given that under the current regulations there doesn't appear to be a clear difference in the degree to which stored telephone and internet data infringe on the privacy of individual citizens; and given that their use in criminal investigation practices is also similar (especially in the case of smartphones), it would seem obvious to harmonize these retention periods.*

Arguably, location records are less intimately linked to the remainder of the data set, however the privacy impact of this element of the data set has been significantly reduced by limiting the type of information required to be retained (eg cell tower location records, rather than triangulated location records), and the volume of records to be retained (call event only, as opposed to continuous records). Additionally, location information can provide important contextual information about communications that is often important for both inculpatory and exculpatory purposes. For example, where a suspect makes a phone call immediately after the time a crime was committed, that phone call may appear

[28] Ministry for Security and Justice, Netherlands Government, *The Dutch implementation of the Data Retention Directive* (2013) 139-40.

suspicious. However, location records showing the phone call was made several suburbs from the scene of the crime would tend to remove that person from suspicion.

The Bill provides for exemptions to be granted so that a shorter retention period may be applied for particular services and types of telecommunications data having regard to law enforcement and security interests, compliance costs and a range of additional factors. Shorter retention periods may also be approved as part of a data retention implementation plan during progress towards full compliance.

The two year retention period, coupled with appropriate implementation, exemption and oversight arrangements, strikes a balance between the law enforcement and national security interests, cost to industry, and the privacy intrusion associated with retaining metadata.

Use of telecommunications data by service providers

The *Privacy Act 1988* and Part 13 of the *Telecommunications Act 1997* (Protection of communications) regulate the use, disclosure and destruction of personal and communications-related information by the telecommunications industry. Accordingly, the Bill does not introduce additional restrictions on how the telecommunications industry uses information in its possession.

In particular, the Bill does not restrict the ability of providers to collect, retain or use information beyond the scope of data retention for business purposes. As noted above, data retention obligations apply to only a limited subset of telecommunications data commonly used by the telecommunications industry. As such, restricting the ability of industry to collect, retain and use other telecommunications data would likely significantly disrupt the operation of many telecommunications services and networks. Additionally, the Bill does not introduce additional requirements on industry to destroy retained data. At present, many providers retain certain types of telecommunications data, such as subscriber and telephony call charge records, for periods far in excess of two years for other business purposes and in compliance with the TCP code; Australian Privacy Principle 11.2 then requires entities to destroy personal information when it is no longer required for a legitimate purpose.

Implementation arrangements

Implementing data retention will require service providers to modify their systems. The extent of these modifications will vary across providers. During the consultation process, industry members advised the Department and Government that an eighteen-month implementation period would significantly reduce their compliance costs. An extended implementation period would, for example, allow companies to align the implementation of data retention solutions with their internal business planning and investment cycles, and by allowing data retention solutions to be incorporated into broader system upgrades.

Law enforcement and security agencies have advised the Department that they support industry members having an appropriate amount of time to fully and properly implement data retention solutions, provided that:

- mechanisms are in place to prevent further degradation to agencies' investigative capabilities during the implementation period, and
- there is scope to work with particular service providers to address the most urgent capability gaps as a priority.

Accordingly, the Bill allows service providers up to 24 months to fully implement data retention capability, while creating a formal implementation plan scheme to support interim measures and progressive implementation.

Commencement period

Data retention obligations will not commence until 6 months after the Bill receives Royal Assent. This period will allow service providers time to develop data retention implementation plans (addressed further below), and to integrate data retention compliance into their internal business plans.

During this period, Item 8 of Schedule 1 of the Bill provides that service providers must not reduce the period for which they retain telecommunications data that will be covered by data retention obligations. This provision prevents any further degradation to agencies' investigative capabilities during this pre-commencement period. There is scope, however, for the CAC to grant exemptions from this requirement. The CAC may consider such exemptions where, for example, a service provider is already in the process of a major system change that is scheduled to come into effect during this 6-month window and data retention capabilities will be built into the new system.

Implementation plans

Proposed new sections 187D to 187J allow a service provider to submit an implementation plan to the CAC for approval, setting out a pathway to full compliance over a period of up to 18 months. When considering a plan, the CAC will be required to consider law enforcement and national security interests, as well as the degree to which the plan reduces the regulatory burden for the provider. Once approved, a plan effectively modifies a provider's obligations under the Act for up to 18 months as outlined in the plan.

The implementation plan process is modelled broadly on the implementation planning arrangements under the *Broadcasting Services Act 1992* for the conversion to digital television, and is intended to:

- allow service providers to develop and implement more cost-effective solutions to their data retention obligations, for example, by aligning the implementation of such solutions with a provider's internal business planning and investment cycles, or by modifying networks or services to allow data to be collected and retained more efficiently
- ensure that service providers achieve substantial compliance with their data retention obligations early in the implementation phase by encouraging interim data retention solutions, for example, by increasing storage capacity for existing databases to approach the two year retention period, or by prioritising the implementation of full data retention capability for some services or kinds of data
- facilitate engagement between industry and Government on the above issues
- provide regulatory certainty for industry during the implementation phase—once approved, a plan may only be varied if both the service provider and the CAC agree,[29] and
- provide certainty for agencies that critical capability gaps will be mitigated in a timely fashion.

There is also no restriction on providers of wholesale telecommunications services providing a data retention service on behalf of their wholesale customers, which would likely increase efficiencies and reduce the cost impacts across the sector.

[29] The CAC is required to consider the same range of matters when deciding whether to agree to a variation of an implementation plan as he or she is required to consider when approving the initial plan.

Data retention implementation plans will complement the availability of exemptions under proposed new section 187K.

Exemptions

Proposed new section 187K will allow the CAC to exempt a specified service provider, or a specified class of service providers,[30] from the data retention obligations, or to vary the provider's obligations. The proposed exemption process is modelled on the current exemption regime for 'interception capability', which is the existing requirement under the TIA Act for providers to develop and implement technical capabilities that enable them to execute interception warrants.

The exemption process will allow the data retention obligation to be tailored appropriately:

- a service might be exempted entirely
- an exemption could apply in respect of a particular type of data, or
- an exemption could reduce the retention period for defined services and/or types of data.

In considering whether to grant an exemption, the CAC is required to consider relevant issues including:

- the interests of law enforcement and national security, for example data relating to a particular service may currently be of relatively lower relevance to investigations
- the cost to a service provider of complying with data retention obligations in relation to the relevant service, and if that cost would be disproportionately high, and
- the objects of the *Telecommunications Act 1997*, which includes matters such as the long-term interests of end-users of carriage services or of services provided by means of carriage services, the efficiency and international competitiveness of the Australian telecommunications industry, and the availability of accessible and affordable carriage services that enhance the welfare of Australians.

The CAC may also take into account the service provider's history of compliance, alternative data retention arrangements that the service provider has identified, and any other relevant issues. Exemptions may also be appropriate for trial services that are not being used or made available to the public, and where data retention capability is being developed but is not yet in place.

The exemptions scheme will complement the provisions for data retention implementation plans. For example, a provider may wish to seek an exemption for some services that are currently of no interest to law enforcement and national security agencies, such as internet television, and submit an implementation plan covering its remaining services.

Enforcement

Data retention obligations will be enforced by the Australian Communications and Media Authority (ACMA) under the existing enforcement regime for industry obligations contained in the Telecommunications Act. This is the same enforcement regime used for interception capability.

---

[30] Although the Bill does not expressly state that the CAC may grant class exemptions, paragraph 111 of the Explanatory Memorandum makes clear that 'the CAC may specify service providers in any way, for example by reference to a class of service providers'. This is consistent with paragraph 23(b) of the *Acts Interpretation Act 1901*, which provides that words in the singular (such as 'specified provider') include the plural ('specified providers').

Industry participants will face pecuniary penalties and infringement notices if they do not comply with data retention requirements. The graduated enforcement options available under the Telecommunications Act include:

- The CAC as the first port of call on exemptions and implementation plans
- In instances where a carrier has failed to comply the CAC can refer the matter to ACMA, and
- ACMA's recourse to apply civil penalties under Part 31 of the Telecommunications Act.

Ultimately, where there is non-compliance with data retention obligations this can lead to the loss of a carrier licence.

Review of the operation of the scheme by this Committee

One of the recommendations of the PJCIS report was that 'the effectiveness of any mandatory data retention regime be reviewed by the PJCIS three years after its commencement.'

Proposed new section 187N of the Bill will require this Committee to review the operation of the data retention scheme three years after the scheme is fully implemented. Because the Bill will only commence six months after Royal Assent followed by an eighteen month implementation phase, this review will be required five years after Royal Assent.

The Department acknowledges that this is a longer period of time than this Committee previously recommended, however this longer period is necessary to ensure that there is an adequate base of evidence about the operation of the scheme for the Committee to consider.

As noted above, service providers will not be required to have fully-compliant systems in place until up to two years after Royal Assent. From that point in time, service providers will then be required to hold data for up to two years, meaning that it may take a further two years (four years after Royal Assent) for many providers to retain the full data set for a full two year period.

The review provisions set out in the Bill will allow the Committee to review the operation of the scheme once it has been fully operational for at least twelve months, ensuring that there is an appropriate evidence base for the review.

A five year review period is consistent with the review period adopted by the European Commission in relation to the former EU Data Retention Directive.

Annual reporting on the operation of the scheme by the Attorney-General

Currently under the TIA Act, the Attorney-General is required to produce, as soon as practicable after each 30 June, an annual report on the use by agencies of their powers under the TIA Act.

The Bill provides that the Attorney-General must prepare a written report on the operation of the data retention regime each year (proposed new section 187P). This report will be included as part of the Annual Report on the *Telecommunications (Interception and Access) Act 1979*, which is currently required under Part 2-8, Part 3-6 and section 186 of the TIA Act.

This will implement the relevant part of Recommendation 43 of the PJCIS report that there should be an annual report to Parliament on the operation of the data retention scheme.

Agencies will continue to be required to report to the Minister on their use of powers under the TIA Act generally. The Attorney-General will continue to be required to produce a report on the use by

agencies of their powers, including accessing telecommunications data, under the TIA Act and table the report in Parliament.

Information security

In its previous report, this Committee recommended that 'data should be stored securely by making encryption mandatory'. The proposed dataset includes information that is privacy-sensitive. As such, the Department agrees that it is important that this information is stored in an appropriate and secure manner.

Existing information security frameworks provide strong protections for the privacy of information held by the telecommunications industry, and will continue to apply to information held in accordance with data retention obligations. The Government has also announced new measures to further strengthen security across the telecommunications sector. The Department's view is that it is preferable to implement a holistic security framework for the telecommunications sector, rather than imposing specific, stand-alone and potentially duplicative security obligations that apply only to a relatively narrow subsection of the information held by industry.

Existing information security frameworks

The *Privacy Act 1988* currently requires regulated entities to adopt a risk-based approach to protecting personal information in their possession from misuse, interference or loss, as well as from unauthorised access, modification or disclosure.[31] The guidelines to the Australian Privacy Principles (APPs) issued by the Australian Information Commissioner explain that entities must consider a range of factors when determining how to protect information they hold, including the amount and sensitivity of the personal information, and the possible adverse consequences for an individual.[32] In particular, the guidelines state that '[m]ore rigorous steps may be required as the quantity of personal information increases'.[33]

Service providers are subject to the data protection obligations contained in Part 13 of the Telecommunications Act. Chapter 4 of the TIA Act sets out the circumstances where agencies may access telecommunications data.

Under section 309 of the Telecommunications Act, the Information Commissioner oversees compliance by telecommunications providers with Part 13 of that Act. This includes monitoring the record-keeping of service providers and ensuring that the grounds for disclosures under Part 13 are recorded by service providers and authorised by the Telecommunications Act and the TIA Act.

Service providers also voluntarily comply with industry codes and standards such as the Payment Card Industry Data Security Standard. The Standard is a proprietary information security standard for organisations that handle branded credit cards from the major card brands including Visa, MasterCard and American Express, and applies over-and-above the above legislative measures.

This Standard is mandated by the card brands. The standard was created to increase controls around cardholder data and to reduce credit card fraud. The standard creates an additional level of protection

[31] Australian Privacy Principle 11.
[32] Australian Information Commissioner, *Australian Privacy Principles guidelines* (2014) [11.7].
[33] Ibid.

for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data.

Telecommunications Sector Security Reforms

The Government has announced that it will implement the Telecommunications Sector Security Reforms (TSSR) recommended by this Committee, and that these reforms will be implemented before data retention is fully implemented.

TSSR is designed to ensure the security and integrity of Australia's telecommunication infrastructure by encouraging ongoing awareness and responsibility for network security by the telecommunications industry, and will extend to provide better protection of information held by industry in accordance with data retention obligations.

TSSR will impose an obligation on service providers to do their best to prevent unauthorised access and unauthorised interference to telecommunications networks and facilities, including where the provider outsources functions.

International comparisons

More than 35 Western countries worldwide have legislated data retention schemes. Many of these countries, including Denmark, France, the Netherlands, the United Kingdom, and Sweden, implemented data retention laws in accordance with the former European Union Data Retention Directive.[34] Others, such as Switzerland and the United States, have implemented data retention laws of their own accord and, in the case of Switzerland, have recently increased the retention period based on their operational experiences. A summary of the data retention and access arrangements in Western countries that the Department is aware have implemented data retention laws is at **Appendix A**.

The most widely implemented data retention scheme is the former EU Data Retention Directive, which was implemented as a response to identified capability gaps following the Madrid and London bombings in 2004 and 2005, respectively. The Directive imposed an obligation on companies to retain specified metadata for up to 2 years. 23 of the 25 member states of the European Union implemented the former Directive.

In 2011, the European Commission prepared an evaluation report on the effectiveness of Data Retention across the EU. That report concluded that the EU should support data retention as a security measure, finding that:

- 'the evidence… attests to the very important role of retained data for criminal investigation',[35] and
- 'These data provide valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Their use has resulted in convictions for criminal offences which, without

[34] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*.
[35] European Commission, *Report from the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive*, 18 April 2011, p.31

data retention, might never have been solved. It has also resulted in acquittals of innocent persons.'[36]

On 8 April 2014 the Court of Justice of the European Union declared that the Directive was invalid.[37] The Court's finding was not because data retention was inherently unconstitutional. Indeed, the Court concluded that, among other things:

- 'data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime'[38]
- 'the retention of data for the purpose of allowing the competent national authorities to have possible access to those data… genuinely satisfies an objective of general interest',[39] and
- 'even though the retention of data… constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that… the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.'[40]

Instead, the Court's judgment was based on the lack of appropriate safeguards and limits within the Directive itself, being that the Directive:

- 'cover[ed], in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception'[41]
- 'fail[ed] to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions'[42] (such matters were left to each member-State of the EU to determine)
- 'require[ed] that those data be retained for a period of at least six months, without any distinction being made between the categories of data… on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned'[43]
- '[did] not provide for sufficient safeguards… to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data',[44] and
- '[did] not require the data in question to be retained within the European Union'.[45]

The invalidation of the Directive has resulted in the annulment of a number of data retention laws in member States where the Directive was implemented, in particular in jurisdictions that had effectively transposed the Directive without incorporating additional, national safeguards. However, the European Commission, and many European countries, are actively working to address the issues identified by the Court. In particular:

---

[36] Ibid, p31.
[37] *Digital Rights Ireland Ltd and Seitlinger* (Court of Justice of the European Union, joined cases C-293/12 and C594/12, 8 April 2014).
[38] Ibid, [43].
[39] Ibid, [44].
[40] Ibid, [39].
[41] Ibid, [57].
[42] Ibid, [60].
[43] Ibid, [63].
[44] Ibid, [66].
[45] Ibid, [68].

- many EU countries have confirmed that their domestic data retention laws will continue to operate unaffected by the Court of Justice's decision, including Sweden, Denmark and France
- a number of other countries have announced amendments to their laws to ensure they are fully compliant with the Court's decision, including the United Kingdom and the Netherlands
- Norway, which had not implemented the Directive, has announced that it is developing new data retention laws
- Germany and the United Kingdom have also announced new data retention laws specifically relating to the retention of critical IP address allocation records by internet service providers.

The Bill has been drafted to ensure that it addresses each of the bases for the Court of Justice's decision. In particular:

- The Bill entirely excludes a large number of communications services where the privacy or compliance impact would be disproportionate to the investigative benefit. Additionally, the Bill entirely excludes telecommunications data relating to a person's web-browsing from the scope of data retention obligations, and significantly limits the volume and detail of location records that are required to be kept.
- The TIA Act, ASIO Act and the Attorney-General's Guidelines strictly control the circumstances in which agencies may access, use and disclose telecommunications data, and impose criminal penalties for the misuse of such information. Additionally, Schedule 2 of the Bill significantly limits the range of agencies permitted to access telecommunications data, and Schedule 3 introduces comprehensive independent oversight of all aspects of the access to, and use and disclosure of telecommunications data by enforcement agencies.
- A consistent, two-year retention period is necessary to ensure that critical information is available, particularly for complex and serious law enforcement, national security and anti-corruption investigations, and is based on both the advice of Australian agencies and the findings of international reviews of data retention laws. Additionally, the Bill expressly allows for the reduction of the period for which telecommunications data must be retained, particularly where there is a limited law enforcement or national security interest in a longer retention period.
- The Privacy Act currently requires service providers to put in place risk-based safeguards against unauthorised access to and misuse of personal information held by industry. Additional, specific controls apply to telecommunications data held by Australian carriers and carriage service providers, and the Australian Government has announced further, sector-wide security reforms.
- The Privacy Act currently regulates the circumstances in which information may be stored outside Australia.

Further discussion on how the Australian implementation of data retention obligations addresses the Court's findings is at paragraphs [66]-[71] and paragraphs [43]-[48] of the Explanatory Memorandum to the Data Retention Bill.

2. Restricting access to stored communications and telecommunications data

This section outlines proposed amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) included in Schedule 2 to the Bill that would affect which agencies are able to apply for stored communications warrants and authorise the disclosure of telecommunications data.

Current framework for agency access

Schedule 2 to the Bill amends two key definitions in the TIA Act: 'enforcement agency' and 'criminal law enforcement agency'. Currently under the TIA Act, an 'enforcement agency' can both apply for a warrant to access stored communications and issue authorisations for the disclosure of telecommunications data.

The term 'enforcement agency' is defined in section 5 of the TIA Act to mean:

(a) the Australian Federal Police; or
(b) a Police Force of a State; or
(c) the Australian Commission for Law Enforcement Integrity; or
(d) the ACC [Australian Crime Commission]; or
(e) the Crime Commission [NSW]; or
(f) the Independent Commission Against Corruption [NSW]; or
(g) the Police Integrity Commission [NSW]; or
(h) the IBAC [Independent Broad-based Anti-corruption Commission of Victoria]; or
(i) the Crime and Misconduct Commission [now the Queensland Crime and Corruption Commission]; or
(j) the Corruption and Crime Commission [Western Australia]; or
(ja) the Independent Commissioner Against Corruption [South Australia]; or
(k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph; or
(l) a body or organisation responsible to the Ministerial Council for Police and Emergency Management - Police; or
(m) the CrimTrac Agency; or
(n) any body whose functions include:
    (i) administering a law imposing a pecuniary penalty; or
    (ii) administering a law relating to the protection of the public revenue.

The agencies listed in paragraphs (a) to (ja) are defined elsewhere in the TIA Act as interception agencies, able to access the content of telecommunications under an interception warrant.

A 'criminal law enforcement agency' is defined in section 5 of the TIA Act as a body referred to in paragraphs (a) to (k) of the definition of enforcement agency. Paragraph (k) of that definition refers to authorities that have been named in the *Telecommunications (Interception and Access) Regulations 1987* (the Regulations). At this time, the only authority named in the Regulations is the Australian Customs and Border Protection Service (Customs).

Paragraph (n) of the definition of enforcement agency is broad and includes a wide range of Commonwealth, State, Territory and local government agencies. Examples of agencies that have accessed telecommunications data can be found in Chapter 3 of the TIA Act Annual Report 2012-13.

Access to telecommunications data under the TIA Act

Section 276 of the *Telecommunications Act 1997* (the Telecommunications Act) prohibits a telecommunications carrier or carriage service provider (C/CSP) from disclosing information relating to the contents or substance of a communication, which includes telecommunications data. The penalty for contravening this provision is imprisonment for two years. However, there are a number of exceptions to this prohibition set out in Part 13 of the Telecommunications Act and Chapter 4 of the TIA Act. Chapter 4 of the TIA Act sets out a regime for enforcement agencies to access telecommunications data.

'Authorised officers' of enforcement agencies may authorise the disclosure of telecommunications data under the TIA Act. Authorised officers are defined in section 5 of the TIA Act to include the following:

i. the head of an enforcement agency; or
ii. a deputy head of an enforcement agency; or
iii. a person who holds an office or position in the enforcement agency that is covered by an authorisation in force under subsection 5AB(1).

Under section 5AB of the TIA Act, an agency head may authorise, in writing, management offices or positions within their agency for the purposes of authorising access to telecommunications data. The enforcement agency must provide a copy of the authorisation to the CAC.

Chapter 4 of the TIA Act sets out the mechanisms for ASIO and the enforcement agencies to authorise the disclosure of data for a variety of lawful purposes.

Section 178 of the TIA Act allows an authorised officer of an enforcement agency to authorise a C/CSP to disclose historic telecommunications data if the disclosure is reasonably necessary for the enforcement of the criminal law. Historic telecommunications data is data that is already in existence when the authorisation is made.

Section 178A of the TIA Act allows an authorised officer of a police force to authorise a C/CSP to disclose historic telecommunications data to assist in locating a missing person.

Section 179 of the TIA Act allows an enforcement agency to authorise a C/CSP to disclose historic telecommunications data if the disclosure is reasonably necessary for the enforcement of law imposing a pecuniary penalty or for the protection of the public revenue.

Section 180 of the TIA Act allows a criminal law-enforcement agency to authorise a C/CSP to disclose prospective telecommunications data for up to 45 days if the disclosure is reasonably necessary for the enforcement of an offence punishable by imprisonment for three years or more. Prospective data is telecommunications data collected in real-time, or close to real-time.

Sections 180A, 180B, 180C, 180D and 180E of the TIA Act govern authorisation of disclosure of telecommunications data in relation to enforcement of the criminal law of a foreign country.

For all of the above disclosure authorisation powers, section 180F of the TIA Act requires an authorised officer to take the privacy impact into account when making any such authorisation.

Under section 182 of the TIA Act, it is an offence to use or disclose telecommunications data obtained under a TIA Act data authorisation except for one of the purposes referred to in that section. These purposes include use or disclosure for national security purposes, the enforcement of the criminal law, the location of missing persons, the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Access to stored communications and issuing of preservation notices under the TIA Act

Chapter 3 of the TIA Act sets out a regime for enforcement agencies to apply for stored communications warrants to access the content of stored communications, such as emails or SMS messages.

Section 108 of the TIA Act prohibits persons from accessing a stored communication held by a C/CSP, except as provided for in that section (such as access under a warrant).

Section 110 of the TIA Act permits an enforcement agency to apply to an issuing authority (an appointed judicial officer or member of the Administrative Appeals Tribunal) for a stored communications warrant to access stored communications content.

The application can be made in relation to the investigation of a 'serious contravention', which is defined in section 5E of the TIA Act to include (amongst other things) offences punishable by imprisonment by three years or more or contraventions rendering an individual liable to pay a pecuniary penalty of 180 penalty units (currently equivalent to $ 30,600, on the basis of $170 per penalty unit) or more.

Under section 116 of the TIA Act, an issuing authority may issue a stored communications warrant if the issuing authority is satisfied, amongst other matters, that information likely to be obtained would be likely assist in the investigation of a serious contravention. The issuing authority must also have regard to:

- the impact on any person's privacy;
- the gravity of the conduct;
- how much the information would assist in the investigation;
- whether other methods of investigation would be available or effective.

Section 133 of the TIA Act makes it an offence to communicate, use, record or give in evidence accessed stored communications, except as provided for in Part 3-4 of the Act.

Part 3-1A of the TIA Act sets out a regime to allow enforcement agencies to issue a notice to a C/CSP requiring it to preserve stored communications it holds for a period of time. Under section 107J of the TIA Act, an enforcement agency can only issue such a notice if it later intends to apply for a stored communications warrant in relation to the investigation of a relevant serious contravention.

Subparagraph 107J(1)(a)(i) of the TIA Act enables any enforcement agency to issue a historic domestic preservation notice to a C/CSP to preserve specified stored communications held by a carrier on the day the notice is noticed.

Subparagraph 107J(1)(a)(ii) allows enforcement agencies that are also interception agencies to issue ongoing preservation notices. Ongoing notices require C/CSPs to keep relevant stored communications held (or obtained) by the carrier for up to 30 days from receipt of the notice.

Amendments regarding stored communications access and telecommunications data access by the Bill

Schedule 2 of the Bill will amend the TIA Act to limit the range of authorities and bodies that can authorise the disclosure of telecommunications data under Chapter 4 of the TIA Act. Schedule 2 of the Bill will also limit the range of agencies that can apply for stored communications warrants or issue preservation notices under Chapter 3 of the TIA Act.

The Bill will limit the range of authorities and bodies that can access telecommunications data and stored communications by amending the definitions of 'enforcement agency' and 'criminal law-enforcement agency' in the TIA Act. A summary of the changes and the policy justification for the measures in Schedule 2 of the Bill is set out below. Further detail is included at pages 66-79 of the Explanatory Memorandum to the Bill.

Proposed changes to which agencies can access telecommunications data

It will continue to be the case that under the TIA Act only 'enforcement agencies' will be able to access telecommunications data, but the ranges of bodies or authorities defined as enforcement agencies will be explicitly and significantly circumscribed.

In principle, any agency or organisation charged by an Australian parliament to enforce laws should have access to the necessary tools to carry out their statutory functions. However, the emerging trend of a wider range of smaller, non-traditional agencies and bodies accessing data without external oversight risks undermining public confidence in the integrity of the regime. In particular, these authorities do not always have internal processes, controls and oversight in place to the same degree as traditional law enforcement agencies.

In 2013 the PJCIS recommended 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.

As a party to the Council of Europe Convention on Cybercrime, Australia has international obligations to make access to telecommunications data available for the investigation of all criminal offences. Article 14(2) of the Cybercrime Convention requires parties to ensure that telecommunications data is available for the investigation of any criminal offence, not just serious offences. Accordingly, amendments that reduce the number of agencies that have access to telecommunications data based on the gravity of the conduct in question would contravene Australia's obligations under the Convention . However, Australia's obligations under the Cybercrime Convention do not preclude reducing the range of agencies that have access to data, because Australia's obligations under the Cybercrime Convention relate only to the availability of telecommunications data for all offences, without specifying the range of agencies which must have access to such data.

Currently, access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits an enforcement agency to authorise a C/CSP to disclose telecommunications data where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue.

The range of agencies that are enforcement agencies and which authorise the disclosure of telecommunications data is broad and includes local councils, State and Commonwealth government departments, agencies such as Centrelink and bodies as the Royal Society for the Prevention of Cruelty to Animals.

The definition of 'enforcement agency' not only confers enforcement agency status on a wide range of authorities and bodies, but also lacks the clarity and specificity of a defined list of agencies falling within the class.

The principle behind the reduction in the number of agencies that can access telecommunications data is that only agencies that have a demonstrated need to access such information, and are subject to appropriate privacy and oversight arrangements, should be permitted to do so. In addition, it should be clear on the face of either the TIA Act or in delegated instruments (such as declarations) which authorities or bodies are enforcement agencies.

Agencies that would no longer be 'enforcement agencies' on the face of the legislation include the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO), the Department of Defence (in particular, the Australian Defence Force Investigative Service), the Department of Foreign Affairs and Trade (in particular, the Passports Office), the Department of Immigration and Border Protection, Racing NSW, the Victorian Department of Environment and Primary Industries, the Wyndham City Council, and RSPCA South Australia.

However, excluded agencies may apply to the Attorney-General following Royal Assent to be declared an enforcement agency. Without seeking to pre-empt either applications or decisions that may be made in future, the Department envisages that some, but not all, of the agencies that have previously accessed telecommunications data in support of the performance of their functions, may be suitable candidates for declaration having regard to the criteria for declaration.

The TIA Act will continue to permit agencies that are not eligible to access telecommunications data in their own right to access such information via a traditional law enforcement agency as part of a joint investigation. This is consistent with current arrangements for joint investigations, and will ensure that, where such access does occur, it occurs within a framework governed by the law enforcement agency's policies, procedures and oversight arrangements.

The controls on access to telecommunications data that already apply to enforcement agencies under the TIA Act will continue to apply. This is consistent with the PJCIS recommendation that, if data retention is implemented, it should be that 'the controls on access to communications data remain the same as under the current regime'.

This means agencies will only be able to access telecommunications data under the TIA Act if it is reasonably necessary for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue. Police forces will also continue to be able to access telecommunications data for the location of missing persons. 'Reasonably necessary' is not a low threshold. It will not be 'reasonably necessary' to access data if it is merely helpful or

expedient. In addition, authorised officers will continue to be required to take into consideration the privacy impact of making the authorisation.

It will continue to be an offence under section 182 of the TIA Act to use or disclose telecommunications data obtained under a TIA Act authorisation, except as provided for in that section. It will also continue to be an offence under the Telecommunications Act for an employee of a C/CSP to disclose telecommunications data except as permitted under Part 13 of the Telecommunications Act or Chapter 4 of the TIA Act.

New section 176A will create a new definition of 'enforcement agency' to replace the definition of 'enforcement agency' currently found in section 5 of the TIA Act. The new definition of enforcement agency in section 176A will include criminal law-enforcement agencies (as set out in new section 110A) and any authority or body declared by the Attorney-General to be an enforcement agency.

When considering whether to declare an authority or body to be an enforcement agency the Attorney-General will be required to consider:

- whether the authority or body has relevant law enforcement functions;
- whether the obtaining of historic telecommunications data would assist the authority or body in performing those functions;
- whether the authority or body is governed by an appropriate privacy regime;
- whether the authority or body will have processes to comply with its obligations under the TIA Act;
- whether the declaration would be in the public interest.

The new definition of enforcement agency replaces the existing open-ended approach of permitting any agency with functions relating to the enforcement laws administering a pecuniary penalty or protection of the public revenue from automatically having access to the power to authorise the disclosure of telecommunications and seek stored communication warrants. Given the existing broad class of agencies which may access the data and stored communications access frameworks, it is not possible to quantify with precision how many agencies will be excluded in the absence of a declaration. However, based on previous use, at least 48 agencies which have previously used this framework will be excluded from the definition on the face of the legislation.

Declarations of authorities or bodies as criminal law-enforcement agencies or enforcement agencies will be disallowable by Parliament, as the declarations will be legislative instruments. The declarations may be revoked by the Attorney-General if he or she is no longer satisfied that the circumstances justifying the declaration remaining in force. In addition, the Attorney-General may impose conditions in the declarations on the exercise of powers to access stored communications or telecommunications data.

The Bill will not change which agencies can access prospective telecommunications data using a prospective telecommunications data authorisation under section 180 of the TIA Act. It will continue to be the case that only criminal law-enforcement agencies will be able to access prospective telecommunications data. Only the interception agencies and Customs will be criminal law-enforcement agencies on the face of the TIA Act under the amended legislation.

Proposed changes to which agencies can seek stored communications warrants and issue preservation notices

Currently, any enforcement agency is eligible to apply for and obtain a stored communications warrant authorising access to stored communications. This leads to the same set of policy challenges in relation to the appropriateness and transparency of which agencies can seek stored communications warrants as for access to telecommunications data, as outlined above.

However, in practice only the interception agencies, Customs, the Australian Competition and Consumer Commission (ACCC) and ASIC have obtained stored communications warrants in recent years. The reason for the lower number of agencies obtaining stored communications warrants is that an agency must be investigating a serious contravention (which generally excludes offences punishable by less than three years' imprisonment) in order to apply for a stored communications warrant. This high threshold for obtaining a warrant excludes most enforcement agencies from such access in practice.

Schedule 2 to the Bill will limit access to stored communications warrants and the ability to issue preservation notices by transferring that power from enforcement agencies to a re-defined set of 'criminal law-enforcement agencies'. New subsection 110A(1) will provide that the following authorities and bodies are 'criminal law enforcement agencies':

(a) the Australian Federal Police
(b) a Police Force of a State
(c) the Australian Commission for Law Enforcement Integrity
(d) the Australian Crime Commission
(e) the Australian Customs and Border Protection Service
(f) the Crime Commission [NSW]
(g) the Independent Commission Against Corruption [NSW]
(h) the Police Integrity Commission [NSW]
(i) the Independent Broad-based Anti-corruption Commission [Victoria]
(j) the Crime and Corruption Commission of Queensland
(k) the Corruption and Crime Commission [Western Australia]
(l) the Independent Commissioner Against Corruption [South Australia], and
(m) an authority or body declared by the Minister to be a criminal-law enforcement agency.

In effect, new section 110A will define all of the interception agencies and Customs as criminal law enforcement agencies. This means that the ACCC and ASIC will no longer be eligible on the face of the TIA Act to access stored communications or issue preservation notices. However, these agencies may apply to the Attorney-General following Royal Assent to be declared a criminal law-enforcement agency. They will continue to be eligible to apply for stored communications warrants or issue preservation notices following Royal Assent until commencement of the limiting amendments, affording a 6 month period to seek a declaration where this may be appropriate.

When considering whether to declare an authority or body to be a criminal-law enforcement agency, the Attorney-General must take into account the following factors:

- whether the functions of the authority or body include investigating serious contraventions;
- whether access to stored communications and prospective telecommunications data would assist the authority or body in investigating those serious contraventions;
- whether the authority or body is governed by an appropriate privacy regime;
- whether the authority or body will have processes to comply with its obligations under the TIA Act;

- whether the declaration would be in the public interest.

The rationale for reducing the number of agencies able to access stored communications or issue preservation notices mirrors that for reducing the number of agencies that can access telecommunications data. The challenges associated with the term 'enforcement agency' in relation to telecommunications data also apply in relation to stored communications access. The term 'enforcement agency' includes a wide range of authorities and bodies, but not all authorities or bodies falling within the meaning of the term need to access stored communications or have appropriate privacy and oversight arrangements.

Only agencies that have a demonstrated need to access the content of stored communications, and are subject to appropriate privacy and oversight arrangements, should be eligible to do so. In addition, it should be clear either on the face of the TIA Act or in secondary legislation (such as declarations) which agencies are eligible to apply for stored communications warrants or issue preservation notices.

These amendments also recognise the greater privacy sensitivity of stored communications as compared to telecommunications data. Unlike telecommunications data, stored communications reveal the content and the substance of a person's communications with others. The Bill therefore continues the current division in the TIA Act between criminal-law enforcement agencies and enforcement agencies, with the difference being that under the amendments proposed in the Bill only criminal-law enforcement agencies will be able to access stored communications content. Enforcement agencies (that are not also criminal law-enforcement agencies) will no longer be able to access stored communications content, but will instead only be eligible to access telecommunications data.

The controls on access to stored communications that currently apply under the TIA Act will not be changed by the amendments in Schedule 2 of the Bill. Agencies will continue to require a warrant to access stored communications. It will continue to be an offence to communicate, use, record or give in evidence accessed stored communications, except as provided for in the TIA Act.

Declarations of 'enforcement agencies' and 'criminal law enforcement agencies'

As noted above, the Bill will permit the Attorney-General to declare an authority or body to be an enforcement agency or a criminal law-enforcement agency.

The Bill specifies a range of factors to which the Attorney-General must have regard in determining whether to declare an agency, including whether the functions of the agency include the enforcement of the criminal law, administering a pecuniary penalty or law protecting the public revenue, whether accessing data would assist in performing those functions, and statutory compliance and privacy arrangements. The Attorney-General, as First Law Officer, is well placed to consider whether an authority or body should be an enforcement agency (or a criminal law-enforcement agency)

The Attorney-General will also have the ability to revoke a declaration should the Attorney-General consider that the reasons supporting the declaration no longer apply.

The declaration process will give the Attorney-General the ability to impose conditions when declaring an authority or body to be an enforcement agency or a criminal law-enforcement agency. This will provide a further ability to restrict access to telecommunications data in a manner consistent with and proportionate to the functions of the agency.

The ministerial declaration process is the most appropriate method to determine which of the wide range of agencies across Australia should be able to exercise the non-interception TIA Act powers. This is because ministerial declarations afford flexibility to take into account changes made to agency structures and functions. Commonwealth, State and Territory governments regularly change the law enforcement responsibilities of agencies through amendments to administrative arrangements orders and Acts of Parliaments. The speed at which such responsibilities can shift means that the availability of TIA Act powers to a particular body also needs to be both responsive and transparent.

For example, a state government may shift responsibility for the enforcement of particular criminal laws under one piece of legislation to another agency or to an entirely new entity. A ministerial declaration would allow the Commonwealth Attorney-General to consider the appropriateness of allowing TIA Act powers that the state government believes are appropriate for the new agency and the Attorney-General may meet such a request in a short period of time so that that agency can undertake its statutory functions with the appropriate tools. By comparison, if changes were only possible by amending the TIA Act, the Act would have to be frequently amended in response to administrative changes across Commonwealth, State and Territory governments. It is therefore appropriate that this particular responsibility rest with the Attorney-General.

3. Oversight

This part of the submission discusses oversight by the Ombudsman in relation to access by agencies to stored communications and telecommunications data introduced by the Bill.

Current oversight of TIA Act powers

The TIA Act and State and Territory legislation currently contains a range of oversight mechanisms in relation to agency use of powers under the TIA Act. These include:

- the Commonwealth Ombudsman oversights Commonwealth agencies in relation to interception of content and all agencies with respect to stored communications.
- the Commonwealth Ombudsman prepares annual reports for the Attorney-General regarding its oversight functions.
- State and Territory Ombudsmen and equivalent authorities oversight telecommunications interception by State and Territory agencies, pursuant to State and Territory legislation (for example, the *Telecommunications (Interception and Access) (New South Wales) Act 1987).*

The Department also compiles annual reports regarding interception, stored communications access and telecommunications data access, which are tabled in Parliament.

Oversight of access to stored communications

The TIA Act currently confers specific oversight functions on the Commonwealth Ombudsman in relation to access by State and Commonwealth enforcement agencies to stored communications.

Section 150 of the TIA Act requires enforcement agencies to destroy information or records obtained by accessing a stored communication if the information or record is not likely to be required for purposes such as the investigation of serious contraventions. Section 150A of the TIA Act requires enforcement agencies to keep documents connected with the issue of preservation notices. Section 151 of the TIA Act requires enforcement agencies to keep documents connected with the issue of stored communications warrants.

Section 152 of the TIA Act empowers the Commonwealth Ombudsman to oversight Commonwealth and State enforcement agencies' compliance with their destruction and record-keeping obligations under sections 150, 150A and 151 of the Act.

In relation to stored communications, the Ombudsman's powers under the *Ombudsman Act 1976* extend to stored communications inspections, as if the inspection were an investigation by the Ombudsman under that Act (TIA Act section 154). The practical effect of section 154 of the TIA Act includes that the Ombudsman has powers to obtain information and documents, examine witnesses and enter premises in relation to its inspections concerning stored communications.

Ombudsman's Annual Report on interception and stored communications records

The Ombudsman must submit Annual Reports on inspections undertaken during the financial year to the Attorney-General (TIA Act sections 84(1), 153(1)). These reports assess compliance with destruction and record-keeping requirements in relation to telecommunications interception by Commonwealth agencies. These reports also assess compliance with destruction and record-keeping requirements in relation to stored communications access by Commonwealth, State

and Territory agencies. The Ombudsman may also report to the Attorney-General at any time about such inspections, and must report at the request of the Attorney-General. A summary of these reports is included in each Annual Report prepared pursuant to the *Telecommunications (Interception and Access) Act 1979*.

The Ombudsman's inspection reports relating to interception must include a summary of inspections, deficiencies impacting on the integrity of telecommunications regime and any remedial action taken or proposed to be taken.

The Act does not specify the content of reports covering the Ombudsman's stored communications annual inspection, other than the results of inspections assessing the destruction and record keeping requirements.

Inspection and record-keeping in relation to telecommunications data

Although agencies are required to keep copies of their authorisations, there are no dedicated inspection requirements regarding telecommunications data access for either the Commonwealth Ombudsman or for State and Territory equivalent authorities. However, Ombudsman annual inspection reports on telecommunications interception and stored communications inspections may also include details of other contraventions of the TIA Act.

Under section 185 of the TIA Act, agencies are required to keep a copy of data authorisations that they make for three years. The TIA Act does not specify any further requirements for enforcement agencies to retain records in relation to the use of powers to access, use or disclose telecommunications data.

Section 305 of the Telecommunications Act requires C/CSPs to retain copies of telecommunications data authorisations made by enforcement agencies for three years. C/CSPs must also keep records of any disclosures of historic telecommunications data made to enforcement agencies under TIA Act data authorisations for three years. Section 306A provides similarly in relation to disclosures by C/CSPs of prospective telecommunications data.

Amendments - new Ombudsman oversight

Schedule 3 of the Bill will enhance the Commonwealth Ombudsman's oversight of stored communications access by agencies. The Bill will also create a new oversight by the Commonwealth Ombudsman of access to telecommunications data by enforcement agencies.

The Bill will insert a new Chapter 4A into the TIA Act to provide a comprehensive record-keeping, inspection and oversight regime by the Commonwealth Ombudsman in relation to:

- the issue of preservation notices by criminal law-enforcement agencies;
- the access to, and dealing with, stored communications by criminal law-enforcement agencies; and
- the access to, and dealing with, telecommunications data by criminal law-enforcement agencies and enforcement agencies.

The proposed oversight regime will be similar to the existing Ombudsman oversight model contained in Division 3 of Part 6 of the *Surveillance Devices Act 2004* (Surveillance Devices Act).

New record-keeping requirements

The PJCIS recommended in 2013 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.

In this context, the PJCIS said (at paragraph 2.34) that 'the Committee strongly supports the need for record-keeping requirements as a means of ensuring meaningful oversight and accountability'.

The Bill will provide for increased document retention requirements by agencies with a view to ensuring that agencies retain appropriate records to enable the Ombudsman to carry out its oversight functions. Currently, agencies are only required to retain limited documents in relation to preservation notices, stored communications warrant applications and telecommunications data authorisations. The proposed new record-keeping requirements will ensure that agencies have relevant records to demonstrate the extent to which their use of powers was appropriate and complied with the requirements set out in that Act.

New section 151 of the TIA Act will comprehensively set out the information or documents that a criminal law-enforcement agency must retain to enable the Ombudsman to inspect the agency's records to determine the extent of its compliance. The records that criminal-law enforcement agencies will be required to keep will include (amongst other things):

- records in relation to the issue and revocation of preservation notices;
- stored communications warrants and documentation associated with application for these warrants and, if applicable, revocation of these warrants;
- records in relation to the use and communication of stored communications warrants;
- records indicating that stored communications information was destroyed as required.

Schedule 3 of the Bill will also amend the documents required to be retained in relation to the access to and use of telecommunications data by enforcement agencies.

Proposed new section 186A of the TIA Act will set out the information or documents that an enforcement agency must retain to ensure that the Ombudsman is able to inspect the agency's records to determine the extent of the agency's compliance with Chapter 4 of the TIA Act. The records that enforcement agencies will be required to keep will include (amongst other things):

- telecommunications data authorisations made by enforcement agencies under sections 178, 178A, 179 and 180, as well as information demonstrating that such authorisations were properly made;
- telecommunications data authorisations made by the AFP in relation to the enforcement of the criminal law of a foreign country under sections 180A or 180B of the TIA Act (and any use of other powers referred to in those sections), and information demonstrating that such authorisations were properly made;
- notices of revocation of prospective telecommunications data authorisations;
- in relation to the AFP – records in relation to the secondary disclosures of telecommunications data to a foreign country for the enforcement of the criminal law of a foreign country under section 180C; and secondary disclosure to Australian agencies of information disclosed for the enforcement of the criminal law of a foreign country under section 180D;

- records indicating that telecommunications data information was properly disclosed according to section 181B;
- records indicating that secondary disclosure of telecommunications data was properly made according the requirements of section 182.

Updating oversight by the Commonwealth Ombudsman

Currently, there is no oversight of agency access to telecommunications data under the TIA Act. In addition, the Ombudsman's oversight role in relation to stored communications is limited to monitoring the compliance by agencies with their record destruction and record-keeping obligations.

The PJCIS considered the issue of oversight of agency use of powers under the TIA Act and recommended 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.

In addition, Recommendation 42 of the PJCIS report recommended that if data retention was implemented, there should be oversight of agency access to telecommunications data by the Ombudsman.

In addition to agencies' new record-keeping requirements, schedule 3 of the Bill will update the Commonwealth Ombudsman's oversight role in relation to stored communications and provide a new role for the Ombudsman, consistent with the PJCIS's recommendations.

The Ombudsman will oversee agency use and access to retained telecommunications data under the TIA Act. This oversight function of the Ombudsman will support accountability concerning agency access to retained telecommunications data under the TIA Act.

This draws on the model contained in Part 6 of the Surveillance Devices Act.

Currently, the emphasis of the Ombudsman's oversight role under Chapters 3 of the TIA Act is on determining agency compliance with record keeping and destruction provisions. The enhanced oversight function proposed in the Bill will enable assessment of an agency's overall compliance with their powers to access and use stored communications and telecommunications data under the TIA Act. The proposed provisions will enable the Ombudsman to provide public accountability as to how agencies have applied their powers under Chapters 3 and 4 of the TIA Act.

The enhanced oversight role given to the Ombudsman in Schedule 3 of the Bill requires that the Ombudsman be given powers to enter agency premises at a reasonable time, inspect the records of agencies and obtain relevant documentation and information to carry out its oversight functions. The Bill will insert these powers. These powers mirror those that the Ombudsman has in its inspection regime in the Surveillance Devices Act.

The Bill will empower the Ombudsman to require an officer of an enforcement agency to provide information to the Ombudsman in writing, and make it an offence to refuse to attend, give information or answer questions when required to do so. The offence will ensure that agency officers do not

hinder the Ombudsman inspection functions by unreasonably refusing to attend, give information or answer questions as required.

The Bill also ensures that the Ombudsman obtains access to documents despite other laws, including the law of any State or Territory to ensure the Ombudsman is able to obtain all information and documents required to carry out the Ombudsman's inspection functions and that agency officers are not prevented by other laws from providing necessary information or assistance.

Reporting by the Ombudsman on inspections

The Bill creates a new public reporting regime in relation to the Ombudsman's oversight functions. The Ombudsman will be required to report on the results of its oversight functions relating to compliance by agencies generally with the requirements of the TIA Act relating to issue of preservation notices, access to stored communications and access to telecommunications data.

The Ombudsman will report to the Attorney-General after the end of each financial year on the results of the Ombudsman's inspections. The Attorney-General must table the report in Parliament within 15 sitting days of receiving it.

The public reporting requirement in the Bill is similar to the public reporting provision that is already in place for Ombudsman reports under section 60 of the Surveillance Devices Act.

Criminal offence to refuse to comply with Ombudsman inspections in relation to telecommunications interception

The Bill makes it an offence for an officer of a Commonwealth agency to refuse to comply with the requirement to attend, give information or answer questions in relation to the Ombudsman's oversight of telecommunications interception.

Proposed subsection 87(6) of the TIA Act mirrors proposed subsection 186C(3) (applicable to stored communications and telecommunications data) in terms of the form of the offence and the applicable penalty. It is also consistent with a similar provision in section 56(6) of the Surveillance Devices Act.

This is the only amendment made by the Bill in relation to the Ombudsman's oversight functions relating to telecommunications interception under Part 2-7 of the TIA Act.

Appendix A—Summary of data retention and access arrangements in Western countries

Note that in relation to the 'Access Method' information column below, in many civil law countries, prosecutors play an investigative role alongside police, in addition to their Australian-style public prosecutor role.

Also note that warrants are generally generic, investigation-level (i.e. authorising data for the purpose of this murder).[46]

Country	Retention period	Access method
Austria	Previously between 8 and 14 months Annulled following the annulment of the EU Data Retention Directive	Internal authorisation
Belgium	Between 12 months and 3 years	Warrant issued by a judicial officer or a public prosecutor
Brazil	6 months for web browsing history 12 months for IP address allocation	
Bulgaria	12 months	Warrant issued by a judicial officer
Cyprus	Previously 6 months Annulled in 2011	Warrant issued by a judicial officer
Czech Republic	Previously between 6 and 12 months. Annulled as a result of the annulment of the EU Data Retention Directive Currently drafting new laws	Internal authorisation
Denmark	12 months Denmark previously required internet service providers to also retain web-browsing information for 1 in every 500 packets sent over the internet. This requirement was removed in mid-2014, following advice from agencies and prosecutors that there were technical difficulties in obtaining useful information from only 0.2% of such traffic. Annulled but will reintroduce in January 2015	Warrant issued by a judicial officer
Estonia	12 months	Prosecutor authorisation
Finland	12 months	No authorisation required for subscriber information. Judge's authority for traffic data.
France	12 months	Authorisation from the Interior Ministry (from 1 January 2015)
Germany	Previously 6 months Annulled in 2010 Draft amendments to Telemedia Act for limited data retention	Internal authorisation
Greece	12 months	Warrant issued by a judicial officer
Hungary	12 months	Internal authorisation
Iceland	6 months	
Ireland	Between 12 and 24 months	Internal authorisation
Italy	12 months for IP address allocation 2 years for telephony	Hybrid – public prosecutor or, in the case of organised crime or counter-terrorism, an internal authorisation.

[46] See Interception of Communications Commissioner's Office, United Kingdom Government, *Evidence for the Investigative Powers Review* (2014) 32.

Country	Retention period	Access method
Latvia	18 months	Judicial authorisation for traffic data. Police authority for subscriber information.
Liechtenstein	6 months	
Lithuania	6 months	Internal authorisation
Luxembourg	6 months	
Malta	Between 6 and 12 months	Internal authorisation
Netherlands	6 months for IP address allocation 12 months for telephony	Hybrid – Internal authorisation for security agencies and less-intrusive law enforcement requests; prosecutorial warrant for more intrusive law enforcement requests.
Norway	6 months Entered into force on 1 January 2015	
Poland	2 years	Internal authorisation
Portugal	12 months	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Romania	Previously 12 months Annulled as a result of the annulment of the EU Data Retention Directive	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Serbia	12 months	Judicial authorisation for traffic data. Internal authorisation for subscriber information.
Slovakia	Between 6 and 12 months Temporarily suspended while under judicial consideration	
Slovenia	Previously 12 months Annulled as a result of the annulment of the EU Data Retention Directive	Internal authorisation
South Africa	3 years	
Spain	Between 6 months and 2 years	Internal authorisation
Sweden	6 months	
Switzerland	6 months Laws before Parliament to increase to 12 months	
Turkey	Between 6 months and 2 years	
United Kingdom	12 months, with extraterritorial application	Internal authorisation for most agencies. However, local authorities require a warrant from a judicial officer.
United States	18 months (telephony only)	Internal authorisation

Appendix B—Number of data authorisations from *Telecommunications (Interception and Access) Act 1979 Annual Report 2012—13*

The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) requires enforcement agencies to report on the number of data authorisations. The following table provides the number of data authorisations in 2012–13. The TIA Act Annual Report can be found at http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Annualreports.aspx

Authorisations[47]	
Authorisations for access to existing information or documents in the enforcement of a criminal law	319,874
Authorisations for access to existing information or documents in the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue	10,766
Authorisations for access to prospective information or documents in the enforcement of a criminal law	7,532
Authorisations for access to existing information or documents for the location of missing persons	895
Authorisations for access to existing information or documents to enforcement of the criminal law of a foreign country	4
Authorisations for access to prospective information or documents to enforcement of the criminal law of a foreign country	1

[47] There is a difference between "authorisations" in the TIA Act and "disclosures" in the ACMA annual report. There is not a one-to-one relationship, where for every one authorisation there is one disclosure. In fact, there will generally be a number of disclosures made in relation to the one authorisation. For example, a senior officer within a law enforcement agency may "authorise" the disclosure of information from a carrier. If the carrier has two or more pieces of information that may be disclosed to give effect to that request, the carrier will then report the number of "disclosures" made pursuant to that authorisation. Fairfax has reported that iiNet said it counted one disclosure as a disclosure of any piece of information and that "searches under an IP address, an email account, phone calls made, and phone calls received would constitute four disclosures". An authorisation will also only be made to each carrier, instead of one authorisation being made to several carriers.

Appendix C—Department's submission to the Senate 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',[48] which is a significantly narrower range of enforcement agencies.

[48] 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.

[THIS PAGE LEFT INTENTIONALLY BLANK]

ATTACHMENT A

Definition of Telecommunications Data

Also known as Metadata, Communications Data and Communications Associated Data

This 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.

Additional case studies

Customs and Border Protection investigation of drug importation

In 2012 Customs and Border Protection arrested a person suspected of illegally importing a marketable amount of pseudoephedrine, which carries a penalty of up to 15 years imprisonment. During the investigation, Customs and Border Protection accessed telecommunications data which confirmed the use of a false name and address to import the pseudoephedrine. Other telecommunications data obtained confirmed the existence of links to other known criminals and provided information about the location of the parties involved.

The use of telecommunications data during this investigation enabled Customs and Border Protection to build a strong case to proceed to prosecution of the alleged offender.

Protection of victims – ACC-led Task Force GALILEE

On 13 April 2011, the ACC Board established the multi-agency Task Force GALILEE to investigate serious and organised investment fraud (SOIF) affecting Australian citizens.

Since 2007, SOIF activities have been identified as impacting on over 2,600 individual victims, including 880 companies, with identified losses in excess of $113 million. These loses relate to an analysis of 183 offshore bank accounts and 165 fraudulent company entities. SOIF is conducted by promoters who spruik fraudulent investments to potential victims using a range of techniques, including cold-calling, email communications and websites.

Telecommunicates data was essential to the work of GALILEE. Telecommunications data provided the foundation in detecting the perpetrators of this crime, as well as identifying the extent of criminal activity and financial losses. Importantly, access to telecommunications data proved critical in enabling the ACC and partners under GALILEE to identify and warn individual victims.

The Task Force was able to quantify the extent of losses to the community arising from serious and organised investment fraud, built on telecommunications data. This knowledge has been used to lead a national education campaign to decrease the number of potential future victims, including through fraud and prevention advice to the elderly, education programs with local bank representatives to promote fraud warnings to rural areas, presenting to key industry bodies such as share registrars on investment and SOIF and liaising with banking agencies for assistance with tracing accounts, and publishing advice on how to protect against investment and Serious and Organised Investment fraud on government websites.

the leading lawyers to government

Sensitive: Legal

Australian Government Solicitor
4 National Circuit Barton ACT 2600
Locked Bag 7246 Canberra Mail Centre ACT 2610
T 02 6253 7000 DX 5678 Canberra
www.ags.gov.au

Canberra
Sydney
Melbourne
Brisbane
Perth
Adelaide
Hobart
Darwin

REPORT

PRIVACY IMPACT ASSESSMENT: PROPOSED AMENDMENTS TO THE *TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979*

15 December 2014

To:
National Security Legal Policy Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

Sensitive: Legal

How is this PIA structured? **3**

Introduction **3**

Information provided and material reviewed 3

Scope of this PIA and contextual background 5

Assumptions made 5

Focus of this PIA **6**

Introduction of new data retention regime for non content data 6

Changes to enforcement body definitions and authorisation arrangements 7

Introduction of new oversight mechanisms in relation to operation of new Part 5-1A and activities of enforcement agencies 7

Privacy impact analysis – privacy implications and analysis of personal information flows **8**

Introduction of new data retention regime for non content data **9**

The entities which are subject to the data retention regime 9

The kind of information to which the data retention regime applies 10

Information or documents proposed to be prescribed under the data retention regime 11

The information to which the data retention regime applies will include personal information 13

Collection of personal information 14

Providing notice of collection 15

Use and disclosure of information to which the data retention regime applies 16

Information quality 16

Security and retention of information to which the data retention regime applies 17

Access and correction 19

Changes to enforcement body definitions and authorisation arrangements **19**

Relevant information-handling aspects of current telecommunications law that are not altered by these changes 19

Broader information-handling obligations that are not altered or otherwise affected by these changes 20

The narrowing effect of these changes – a privacy positive 21

Introduction of new oversight mechanisms in relation to operation of new Part 5-1A and activities of enforcement agencies **24**

Oversight - operation of new Part 5-1A 24

Oversight – activities of agencies 24

Overall effect and impact of these changes and related recommendations **25**

Sensitive: Legal

REPORT

PRIVACY IMPACT ASSESSMENT: PROPOSED AMENDMENTS TO THE *TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979*

1.1. The Attorney-General's Department (the Department) has asked us to conduct a privacy impact assessment (PIA) for proposed amendments to the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) relating to data retention. The proposed amendments are set out in the following draft Bill: Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the draft Amendment Bill).[1]

HOW IS THIS PIA STRUCTURED?

1.2. This PIA is divided into the following sections:

- The **introduction** section outlines the information provided to us by the Department and the material we have reviewed, sets out the scope and contextual background of this PIA and notes the assumptions we have made in preparing this PIA.
- The **focus of this PIA** section describes what the draft Amendment Bill will do.
- The **privacy impact analysis – privacy implications and analysis of personal information flows** section examines the changes that will be made by the draft Amendment Bill from a privacy perspective, by identifying and examining relevant data flows (including data that comprises personal information) and analysing the effect and impact of these changes having regard to the existing and ongoing privacy obligations of the various government and private sector entities that will be subject to these changes.

These sections are followed by **a summary of our views on the overall effect and impact of these changes and related recommendations** on the various matters discussed in this PIA.

INTRODUCTION

Information provided and material reviewed

1.3. To prepare this PIA we have considered the Department's initial instructions dated 22 October 2014 and the terms of the draft Amendment Bill. In addition, we have

---

1 This PIA was initially prepared with reference to a draft version of the draft Amendment Bill. Following the introduction of the draft Amendment Bill into Parliament on 30 October 2014 the Department provided us with a copy of the Bill as introduced. The PIA has been updated to reflect the Bill as introduced. While the draft Amendment Bill reflects proposed amendments to both the TIA Act and the *Telecommunications Act 1997* (Cth) (the Telecommunications Act), we note that the amendments to the Telecommunications Act set out in Part 2 of Schedule 1 to the Bill are not of a substantive nature. To this end, this PIA focuses on the amendments to the TIA Act, although mentions the operation of the Telecommunications Act (including proposed amendments to the Telecommunications Act) in passing as relevant.

Sensitive: Legal

reviewed the following documents, as provided or suggested to us by the Department on 22, 23 and 28 October 2014:

- the *Privacy Impact Assessment – Preliminary Report – Telecommunications (Interception and Access) Act 1979* prepared for the Department by Information Integrity Solutions in December 2011 (the earlier PIA)
- the 2011 European Commission *Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*
- the 2013 Parliamentary Joint Committee on Intelligence and Security *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (the PJCIS report), in particular Chapter 5 relating to data retention
- the consultation comments on the draft Amendment Bill provided to the Department by the Office of the Australian Information Commissioner (OAIC) on 17 October 2014 (OAIC consultation comments)
- the draft *Statement of compatibility with human rights* prepared by the Department for the draft Amendment Bill[2]
- the draft *Telecommunications (Interception and Access) Amendment (Data Retention) Regulation 2014* (the draft Amendment Regulation) which describes the proposed dataset to which these amendments are intended to apply.[3]

1.4. We have also had regard to the various matters discussed and further instructions provided during our meetings with officers from the Department on 23 and 24 October 2014.

1.5. More broadly, we have examined and considered the relevant operation of the *Privacy Act 1988* (Cth) (the Privacy Act) and the TIA Act. We have also referred to the *Guide to undertaking privacy impact assessments* issued by the OAIC in May 2014 (the OAIC guide).

1.6. Given the time available, other than at a very high level (as described further below in paras 1.66-1.68), it has not been possible for us to examine and consider the potential relevance of the other Commonwealth, State and Territory legislation that imposes a range of privacy, secrecy and confidentiality obligations on the various government and private sector entities that will be subject to the changes to be made under the draft Amendment Bill.

1.7. In addition, because of time constraints but more significantly because we consider that it goes beyond the scope of the issues raised directly by the draft Amendment Bill, we have not undertaken any detailed research on the broader privacy issues that may be raised by proposals concerning the general subject matter of

2 Being the version provided to us by the Department by email on 22 October 2014.

3 We have prepared this PIA with reference to the following version of the draft Amendment Regulation: I14KM204.v06.docx 28/10/2014 11:56 AM. An early description of the proposed dataset to which these amendments are intended to apply was provided to us by the Department by email on 23 October 2014.

telecommunications data retention (see also our comments below in paras 1.11-1.12).

Scope of this PIA and contextual background

1.8. The focus of this PIA is the effect and associated privacy implications of the changes to the current operation of the TIA Act that are proposed to be made by the draft Amendment Bill. It has been prepared with reference to the instructions we have received from the Department about the settled policy position of the Government as reflected in the draft Amendment Bill.

1.9. The purpose of this PIA is not to identify possible amendments to the draft Amendment Bill but to analyse and make observations concerning the potential impact of the Bill as drafted on the privacy of individuals.

1.10. This PIA has been prepared against the background of the earlier PIA, the PJCIS report and the recommendation in the OAIC consultation comments that the Department obtain a further PIA in relation to the draft Amendment Bill. Noting that both the earlier PIA and the PJCIS report relate to a much broader tranche of proposed reforms than are reflected in the draft Amendment Bill, it is neither necessary nor appropriate for this PIA to examine all of the matters addressed in these earlier documents. Similarly, to the extent that the OAIC consultation comments identify and discuss broader policy and legal matters that are not raised directly by the draft Amendment Bill, we have not examined these matters further in this PIA.

1.11. As the earlier PIA makes clear, and as is acknowledged in the PJCIS report, there are a host of significant privacy issues that are relevant to the current operation of the TIA Act. They are also relevant to any potential reforms that are proposed to be made either to the TIA Act and related legislation or which otherwise concern the handling (including the retention) of telecommunications data.

1.12. However, as noted above, this PIA focuses only on the amendments to the TIA Act as set out in the draft Amendment Bill. Many of the significant privacy issues and challenges which exist in the broader operational context of regulating telecommunication services and the handling of associated data, as identified in the earlier PIA and the PJCIS report, are not raised by the types of amendments that will be made by the draft Amendment Bill. This is because only relatively limited aspects of the current regulatory regime set out in the TIA Act and related legislation will be changed under these amendments.[4] In all other respects, the current operation of the TIA Act and related legislation will remain unchanged. This PIA does not examine the broader operation of the current legislative regime.

Assumptions made

1.13. We have prepared this PIA on the assumption that the TIA Act will be amended as is proposed under the draft Amendment Bill. For this reason, the comments we

[4] This point is illustrated further by the breadth and scope of the changes relating to the introduction / revision of the definitions of 'criminal law-enforcement agency' and 'enforcement agency', as discussed further in paras 1.69-1.78 below.

make and the conclusions we reach in this PIA should be taken to apply only to the amendments as currently proposed (unless we confirm otherwise). If the TIA Act is amended differently to what is currently proposed under the draft Amendment Bill, then we also suggest that the Department obtain a further or updated PIA to address the effect of these subsequent changes.

1.14. This PIA also assumes that the various government and private sector entities that will be subject to the changes to be made under the draft Amendment Bill are otherwise aware of, and comply with, the privacy, secrecy and confidentiality obligations that currently apply to their day-to-day handling of information and documents including personal information. Related to this, our comments below focus only on the potential privacy impacts of the changes to the TIA Act reflected in the draft Amendment Bill, rather than on the potential privacy impacts of other actions that these entities may potentially take in purported compliance with the TIA Act (including where these other actions have some broad association with, but do not form part of, actions that will need to be taken to comply with these amendments).

FOCUS OF THIS PIA

1.15. This PIA relates only to the substantive changes that will be made to the TIA Act by the draft Amendment Bill. We have identified 3 main changes in this context, which are each described below.

Introduction of new data retention regime for non content data

1.16. Part 1 of Schedule 1 to the draft Amendment Bill will insert a new Part 5-1A into Chapter 5 of the TIA Act. Part 5-1A is headed 'Data retention' and contains provisions relating to:

- imposing obligations on service providers[5] to keep information and documents comprising or recording non content data[6] (Div 1)
- the making of data retention plans by service providers and the effect of those plans (Div 2)
- exempting service providers from obligations under this Part (Div 3)
- miscellaneous matters associated with the operation of this Part (Div 4).

---

5 A 'service provider' is a person who operates a service to which new Part 5-1A applies (see @187A of the draft Amendment Bill). The introduced Bill provides that a relevant service is 'a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both; and (b) it is a service: (i) operated by a carrier; or (ii) operated by an internet service provider (within the meaning of Schedule 5 to the *Broadcasting Services Act 1992*); or (iii) of a kind prescribed by the regulations; and (c) the person operating the service owns or operates, in Australia, infrastructure that enables the provision of any of its relevant services; but does not apply to a broadcasting service (within the meaning of the *Broadcasting Services Act 1992*)' (see @187A(3) of the draft Amendment Bill). This provision needs to be read together with the definition of 'carrier' in s 5(1) of the TIA Act.

6 We use the phrase 'non content data' here to refer to the information and documents which service providers are obliged to retain under @187A.

Sensitive: Legal

1.17. The intended operation of Div 1 is most relevant to the issue of assessing the potential privacy implications of Part 5-1A.[7] The practical operation of relevant clauses within this Division is analysed below.

Changes to enforcement body definitions and authorisation arrangements

1.18. Part 1 of Schedule 2 to the draft Amendment Bill will amend the current provisions in the TIA Act that relate to enforcement agencies accessing stored communications under warrant[8] and accessing telecommunications data.[9] As we understand it, the non content data that will be required to be retained under new Part 5-1A will be 'telecommunications data' to which Chapter 4 of the TIA Act applies but will not fall within 'stored communications' to which Chapter 3 of the TIA Act applies.[10] In both instances, as discussed further in the third part of this PIA below, these amendments have a narrowing effect.

1.19. Under the proposed amendments, the capacity to apply for a warrant to access stored communications will be limited to agencies which are 'criminal law-enforcement agencies' as defined.[11] The new definition names various specific agencies as 'criminal law-enforcement agencies'. It also provides a mechanism for other agencies to request a declaration from the Attorney-General so as to become 'criminal law-enforcement agencies'. Detailed criteria are prescribed in relation to the making of any such declaration.

1.20. The 'criminal law-enforcement agencies' amendment is also relevant to the types of agencies that will be able to access telecommunications data going forward. Under the proposed amendments, a new definition of 'enforcement agency' is inserted. It includes 'criminal law-enforcement agencies' and agencies declared by the Attorney-General to be 'enforcement agencies'. Again, detailed criteria are prescribed in relation to the making of any such declaration.

Introduction of new oversight mechanisms in relation to operation of new Part 5-1A and activities of enforcement agencies

1.21. The draft amendment Bill contains provisions that are directed generally at ensuring monitoring and reporting in relation to the operation of new Part 5-1A. The miscellaneous matters associated with the operation of this Part (set out in Div 4, as noted above) require the PJCIS to conduct a review of the Part's operation at a

---

7 The data retention plans for which provision is made in Div 2 are intended to enable service providers where necessary to transition from their current record keeping practices to full compliance with the data retention regime within 18 months, and are not further discussed in this PIA.

8 See Part 3-3 of Chapter 3 of the TIA Act.

9 See Part 4-1 of Chapter 4 of the TIA Act.

10 We also note in this regard the operation of s 172 of the TIA Act, which makes it clear that Divs 3, 4 and 4A of Part 4-1 of Chapter 4 of the TIA Act (relating to accessing telecommunications data) do not permit the disclosure of 'information that is the contents or substance of a communication … [or] a document to the extent that the document contains the contents or substance of a communication'.

11 See proposed new s 110A of the TIA Act.

Sensitive: Legal

specified future time and provide a copy of its review report to the Minister[12] and require the Minister to prepare a (depersonalised) annual report on the operation of the Part.[13] In addition, a new function is conferred on the Australian Communications and Media Authority (ACMA) under the Telecommunications Act to report to the Minister on the costs of compliance with the requirements of this Part.[14]

1.22. Part 1 of Schedule 3 to the draft Amendment Bill will insert a new oversight regime applying to the actions of both criminal law-enforcement agencies and enforcement agencies. A new specific oversight function is conferred on the Commonwealth Ombudsman (the Ombudsman).

1.23. Under the proposed amendments:

- the chief officers of criminal law-enforcement agencies and enforcement agencies will be obliged to keep specified types of records (new Part 3-5)
- the Ombudsman will be obliged to inspect the records of criminal law-enforcement agencies and enforcement agencies to determine the extent to which such agencies are complying with their respective obligations under the TIA Act (@186B)
- the Ombudsman will have the power to obtain relevant information from agency officers (@186C) and to give such information to relevant State or Territory authorities when it has been obtained from a State or Territory agency officer (@186F)
- the Ombudsman must provide an annual report to the responsible Minister in relation to inspections conducted under @186B.

1.24. We note that the earlier PIA, the PJCIS report and the OAIC consultation comments each made comments about the need to ensure that appropriate oversight mechanisms are included in any proposed legislative amendments as a means of ensuring and enhancing privacy protection.

1.25. We make some further comments below about the privacy-enhancing implications of the various new oversight mechanisms as set out in the draft Amendment Bill.

PRIVACY IMPACT ANALYSIS – PRIVACY IMPLICATIONS AND ANALYSIS OF PERSONAL INFORMATION FLOWS

1.26. In this section we identify and analyse the privacy implications arising from the introduction of the amendments proposed in the draft Amendment Bill. We refer extensively to the Australian Privacy Principles (APPs) set out in Schedule 1 to the Privacy Act. Where we omit discussion of a particular APP in relation to the proposed amendments, it is because the draft Amendment Bill will not make any change to the law in a way that would engage the APP. This means, for example,

12 See @187N.

13 See @187P.

14 See proposed amendment to current s 105(5A) of the Telecommunications Act described in Part 2 of Schedule 1 to the draft Amendment Bill.

Sensitive: Legal

that none of APP 7 (direct marketing), APP 8 (cross border disclosure of personal information) or APP 9 (government related identifiers) are discussed in this PIA. There is nothing in the draft Amendment Bill that engages any of these APPs.

INTRODUCTION OF NEW DATA RETENTION REGIME FOR NON CONTENT DATA

The entities which are subject to the data retention regime

1.27. The new data retention regime will apply to 'service providers'. @187A(1) of the draft Amendment Bill provides that a service provider is a person who operates a service to which new Part 5-1A applies. Such a service is 'a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both; [that is] is a service: (i) operated by a carrier; or (ii) operated by an internet service provider (within the meaning of Schedule 5 to the *Broadcasting Services Act 1992*); or (iii) of a kind prescribed by the regulations; [where] the person operating the service owns or operates, in Australia, infrastructure that enables the provision of any of its relevant services' (see @187A(3)). It does not include a broadcasting service within the meaning of the *Broadcasting Services Act 1992* (see @187A(3)). The definition of carrier in s 5(1) of the TIA Act includes 'carriage service providers', a term defined in the Telecommunications Act in a way which includes persons supplying a listed carriage service to the public over a network.[15]

1.28. A threshold consideration is whether the service providers to which the new regime will apply are entities which are required to comply with the Privacy Act. The Privacy Act applies to 'APP entities', defined in s 6 of that Act to mean an 'agency' or an 'organisation'. We understand from discussions with officers of the Department that the vast majority of service providers will be organisations within the meaning of the Privacy Act[16] and thus subject to the Privacy Act. However, we understand there are a small number of service providers that may be a small business operator within the meaning of s 6D of the Privacy Act, and for that reason may not be required to comply with the Privacy Act.

1.29. It may be possible for the TIA Act to deem all service providers to whom the data retention obligations apply to be organisations for the purposes of the Privacy Act. Specific legislative amendment would be required in this context. However, we understand from our discussions with officer of the Department that the Government has decided not to take this approach. We note that whilst some service providers may not be subject to the Privacy Act:

— All carriage service providers within the meaning of the Telecommunications Act are required to observe and comply with the Communications Alliance *Telecommunications Consumer Protections Code* (the Code). The Code is

15 For the definition of 'carriage service provider' see s 87 of the Telecommunications Act and the various associated definition provisions which must be considered to have a comprehensive understanding of whether a particular entity is a carriage service provider. A listed carriage service is defined in s 16 in a way that includes services from point to point within Australia or from a point outside and within Australia.

16 See the definition of 'organisation' in s 6C.

Sensitive: Legal

registered under Part 6 of the Telecommunications Act by the ACMA, which has powers to enforce compliance. A key principle enshrined in the Code is that consumers 'will enjoy open, honest and fair dealings with their Supplier, *and have their privacy protected*' (our emphasis), and several provisions of the Code relate to protection of privacy.

— The functions of the Telecommunications Industry Ombudsman (TIO) include investigating and facilitating the resolution of complaints about any interference with the privacy of an individual by a telecommunications provider, both in terms of non-compliance with applicable privacy requirements under the Privacy Act (such as the APPs) and also breach of any applicable industry specific privacy standards. Most service providers will be within the jurisdiction of the TIO, and if an individual believes their privacy has been breached and is unable to resolve the matter with the service provider, they will be entitled to seek the assistance free of charge from the TIO through its dispute resolution scheme.

1.30. The following analysis proceeds on the assumption that the relevant service provider must comply with the Privacy Act.

The kind of information to which the data retention regime applies

1.31. The scope of the new data retention regime is restricted under @187A(1) to collection and retention of information of a kind that is prescribed under the regulations, or documents containing that information, relating to a relevant service operated by the service provider.

1.32. The kinds of information that may be prescribed are limited, adopting the description given in the draft *Statement of compatibility with human rights*, to information about the process of communications, as distinct from their content. There are 2 ways in which the kinds of information that may be prescribed are limited.

1.33. First, @187A(2) provides that the kinds of information must relate to one or more of a number of specified things. These things relate to:

— identifying characteristics of a subscriber, an account, a telecommunications device or another relevant service (paragraph (a)), or

— the source or destination of a communication, the date, time and duration of a communication or of its connection to a relevant service, the type of communication or relevant service used in connection with the communication and the location of equipment, or a line, used in connection with a communication (paragraphs (b)-(f)).

1.34. Secondly, @187A(4) provides that @187A does not require a service provider to keep, or cause to be kept, the following:

— information that is the contents or substance of the communication

— information that states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider and was obtained by the service provider only as a result of providing the service (which the note indicates 'puts beyond doubt

Sensitive: Legal

that the regulation making power cannot be used to require service providers to keep information about subscribers' web browsing history')[17]

- information to the extent that it relates to a communication carried by means of another relevant service operated by another service provider and using the relevant service, or a document to the extent that the document contains such information
- information that the service provider is required to delete because of a determination made under s 99 of the Telecommunications Act, or a document to the extent that the document contains such information, or
- information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected.

The information described in the first 2 dash points is mentioned for illustrative purposes in our discussion below.

Information or documents proposed to be prescribed under the data retention regime

1.35. Officers of the Department have advised us that it is intended that the draft Amendment Regulation will be available for public comment and consideration by the Parliament at the same time as the draft Amendment Bill. As noted above, we have been provided with a copy of the draft Amendment Regulation which describes the proposed dataset to which these amendments are intended to apply.

1.36. The information or documents which it is proposed are to be retained comprise each of the categories of information identified in @187A(2). A more particular description of the information to be retained is provided in respect of each category, as follows:

Kinds of information to be kept		
Item	**Matters to which information must relate** **Column 1**	**Information** **Column 2**
1	The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: (i) any name or address information; (ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the

[17] We note in this context the terms of s 172 of the TIA Act – see further fn 10 above. This part of @187A(4) goes beyond the scope of s 172 by referring to web browsing.

Sensitive: Legal

Kinds of information to be kept		
Item	**Matters to which information must relate** **Column 1**	**Information** **Column 2**
		relevant service, or to any related account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service, or any related account, service or device; Examples: When an account has been enabled or suspended, a relevant service has been enabled or suspended or is currently roaming, or a telecommunications device has been stolen. (f) any information about metrics of the relevant service or a related account, service or device. Examples: Bandwidth, upload and download volumes.
2	The source of a communication	Any identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.
3	The destination of a communication	Any identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.
4	The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.
5	The type of a communication or of a relevant service used in connection	The following: (a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. (b) the type of the relevant service;

Sensitive: Legal

Kinds of information to be kept		
Item	**Matters to which information must relate Column 1**	**Information Column 2**
	with a communication	Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. Examples: Call waiting, call forwarding, bandwidth allowances. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c) of the Act.
6	The location of equipment, or a line, used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the start of the communication; (b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.

1.37. The matters described in this table, consistent with @187A(4), do not relate to the content of communications nor do they require the retention of internet browsing history. However, some of the language used in the descriptions is quite broad so may potentially be imprecise or unclear (for instance 'status of' the account and 'any identifiers of'). To the extent possible, the matters should be described in a way, and supported by detailed extrinsic material, that enables service providers and members of the public to be able to clearly understand what information is required to be retained.

The information to which the data retention regime applies will include personal information

1.38. Personal information is defined in the Privacy Act to mean:

> …. information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

1.39. It is clear that the data retention obligation is intended to, and does, relate to personal information within the meaning of the Privacy Act. If a subscriber is an individual, then at least some of the kinds of information which may be prescribed (referred to in @187A(2)) will clearly be personal information relating to that subscriber.

Sensitive: Legal

1.40. If neither the subscriber nor the person receiving a communication are an individual (for instance, they are a corporation), the prescribed information may nevertheless be personal information because the individuals associated with the relevant communication are reasonably identifiable. In such cases, subscriber identity information together with other information such as the source, destination, time and duration of the communication and location of the relevant telecommunications devices, could be expected to enable the individuals using the relevant service for the particular communication to be identified when that information is linked with other information.

1.41. The limitations imposed under @187A(4) make it clear that the data retention obligation is not intended to apply to the content of a communication or information that would reveal web browsing history. This limits the extent to which the personal information concerned may be sensitive information within the meaning of the Privacy Act. Sensitive information is defined under s 6 of the Privacy Act to include, among other things, health information, information about a customer's racial or ethnic origin, political opinions, religious beliefs or affiliations or sexual orientation or practices. There are special requirements under the Privacy Act with respect to handling this kind of personal information.

1.42. There is nevertheless some potential for the personal information that is required to be retained under the proposed amendments to be sensitive information in some cases. An example includes where:

- The subscriber, who is an individual, calls a support group for individuals with a particular sexual orientation. Information which identifies the individual and the particular support group may be sensitive information on the basis it comprises information about the individual's sexual orientation.

1.43. Some of the information required to be kept as part of the data retention regime may not be personal information. For instance, an individual may not be reasonably identifiable from information about the type of communication or type of relevant service used in connection with the communication.

1.44. However, as the Australian Information Commissioner's APP Guidelines note at paragraph B85, whether an individual is 'reasonably identifiable' from particular information will depend on a range of considerations, including the nature and amount of information, the circumstances of its receipt, who will have access, whether it is possible for the APP entity that holds the information to identify the individual and, if the information is publically released, whether a reasonable member of the public who accesses that information would be able to identify the individual. While a member of the public might not be able to link individuals to certain kinds of information required to be retained, it is likely that service providers will in many cases be able to link individuals to particular pieces of information they are required to retain from other information they possess.

Collection of personal information

1.45. APP 3 imposes limits on the collection of personal information by APP entities. Of particular relevance in the present circumstances, APP 3.2 requires that an APP

entity that is an organisation must not collect personal information (other than sensitive information[18]) unless the information is reasonably necessary for one or more of its functions or activities.

1.46. The effect of @187A(6) is that a service provider must separately 'create' information of the kind prescribed if it is not created by operation of the relevant service. The imposition of this obligation may therefore potentially require collection of information additional to that which the service provider would otherwise collect i.e. which might not be reasonably necessary for one or more of its functions or activities.

1.47. However, officers of the Department have informed us that the kind of information that may be prescribed does not go beyond that which service providers are already generating to provide services, albeit that some service providers may not be recording the information or keeping it for very long. The requirement to create information is intended to ensure information already generated by service providers which is of a kind that is prescribed is captured and retained. On this basis, the effect of @187A(6) would not be to require the collection of additional information now, but to ensure that information presently collected continues to be collected into the future.

Providing notice of collection

1.48. APP 5 requires APP entities, at or before the time or as soon as practicable after they collect personal information about an individual, to take such steps as are reasonable to notify the individual of the matters specified in subclause 5.2 as are reasonable in the circumstances, or to otherwise ensure the individual is aware of any such matters. This obligation applies to any collection of personal information, regardless of whether the information is collected directly from the individual, and will therefore apply with respect to the collection by service providers who are APP entities of personal information required to be retained under the data retention regime.

1.49. Assuming that the kind of information that may be prescribed does not go beyond that which service providers are already generating to provide services, the introduction of the data retention regime should not require service providers to make significant changes to their current notification practices in compliance with APP 5. What will be important is that service providers accurately inform subscribers of the kind of information require to be collected to meet their data retention obligations, and of the statutory requirements imposed upon them to collect and in certain circumstances disclose data. To this extent, existing APP 5 notices will require amendment.

---

18 With respect to sensitive information, the effect of APP 3.3 and 3.4(a) in the particular circumstances here is that an organisation within the meaning of the Privacy Act will be permitted to collect sensitive information to the extent it is required or authorised by or under the data retention regime.

Sensitive: Legal

Use and disclosure of information to which the data retention regime applies

1.50. APP 6.1 provides that if an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless the individual consents or APP 6.2 or 6.3 apply. Relevantly, APP 6.2(b) provides for use or disclosure of information 'required or authorised by or under an Australian law or a court/tribunal order'.

1.51. The data retention regime does not make any changes to the requirements imposed on service providers with respect to use and disclosure of information, except to the extent keeping information for a defined period as required under the regime can be characterised as a use.[19] No amendments are being made to ss 174 and 177 which provide for voluntary disclosure in defined circumstances,[20] and service providers will still be required to disclose information, including information kept as required under the data retention regime, when provided with an authorisation under the TIA Act.[21]

Information quality

1.52. APP 10 requires an APP entity to take such steps (if any) as are reasonable in the circumstances to:

- ensure that the personal information that the entity collects is accurate, up to date and complete (10.1), and
- ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant (10.2).

1.53. The data retention regime contains no provisions that will directly affect the manner in which APP entities meet these requirements. However, the requirement to retain data for 2 years, and to retain a more limited subset of that data for longer (as discussed below), will have an impact.

1.54. @187C(1)(a) requires information about, or a document containing information about, a matter of a kind described in @187A(2)(a) (ie identifying characteristics of a subscriber, an account, a telecommunications device or another relevant service) to be retained until 2 years after the closure of the account to which the information or

---

19 This aspect of the regime is discussed below.

20 We note that s 177 makes provision for voluntary disclosure to an enforcement agency if the disclosure is 'reasonably necessary for the enforcement of the criminal law' or 'reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue'. The terms of these provisions are clearly based on parts of the Information Privacy Principles formerly contained in the Privacy Act, which have been replaced by the APPs.

21 As discussed below, the draft amendment Bill will make changes to which bodies in the future will be able to issue an authorisation.

Sensitive: Legal

document relates.[22] We understand the kind of information to be prescribed in the regulations will include both current and historical information with regard to these matters.

1.55. This means a service provider will be required to retain historical information about matters such as the name and address of a subscriber, billing information, their contact details, and information about a telecommunications device the subscriber used for the account, but no longer uses. This will have implications for the service provider with respect to fulfilling its obligations under APP 10.2. The service provider will need to ensure that the historical information is kept in a way that does not allow that information to be confused with current information. It will also be necessary for the service provider to keep accurate records of when particular telecommunications devices were used with the account over time, so that any information disclosed in that regard (for instance, in response to an authorisation under the TIA Act) is accurate.

1.56. @187C(1)(b) provides that the period other kinds of information which may be prescribed under @187A is to be retained is 2 years starting from when the information came into existence. As the other kinds of information relate to particular communications at a point in time, and the information will therefore be historical in nature, there would not appear to be a risk this information could be confused with current information.

Security and retention of information to which the data retention regime applies

1.57. APP 11 requires an APP entity holding personal information to:

- take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss and from unauthorised access, modification or disclosure (11.1), and
- if the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity, it is not contained in a Commonwealth record and the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information, take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de identified (11.2).

1.58. The data retention regime does not impose any particular requirements with regard to security of the information required to be retained by service providers. However, the very purpose of the regime is to require the retention of particular kinds of information for a defined period. This means that even if a service provider no longer needs the information for any purpose, it will be required to retain it for the duration of the period specified in the TIA Act (as amended), and will need to ensure the information is secure throughout that period. This increases the risk of the security

[22] We note that @187C(2) provides that the regulations may prescribe in relation to specified matters of a kind described in @187A(2)(a) that the period is 2 years from when the information came into existence, rather than 2 years after the account is closed.

Sensitive: Legal

of the data being compromised, to the extent that, but for the data retention requirement, the data would not be retained.[23] We understand from our discussions with the Department that, in practice, a 2 year retention period in respect of telephony services will not require providers to keep many elements of the data set for a longer period than they currently retain the data for their own business purposes. We further understand that the 2 year retention period will have a more variable impact in relation to internet-related services, and will require providers to keep some data sets for longer than they are currently kept. The Department has noted in its instructions to us that all elements of the data required to be retained are currently retained by one or more telecommunications providers; however we are instructed that the current retention practices and periods vary between providers.

1.59. @187C(1) sets out the period for which a service provider must keep information or a document under @187A, as follows:

> (a) if the information is about, or the document contains information about, a matter of a kind described in paragraph @187A(2)(a)—the period:
>
> (i) starting when the information or document came into existence; and
>
> (ii) ending 2 years after the closure of the account to which the information or document relates; or
>
> (b) otherwise—the period:
>
> (i) starting when the information or document came into existence; and
>
> (ii) ending 2 years after it came into existence.

1.60. @187C(1)(a) requires that the kinds of information identified in @187A(2)(a) (ie identifying characteristics of a subscriber, an account, a telecommunications device or another relevant service) be retained for 2 years from when the relevant account is closed. This information will therefore be required to be retained for potentially far longer than 2 years.

1.61. The PJCIS recommended that data subject to a mandatory data retention regime be required to be retained for no more than 2 years. There is naturally a concern that the longer the period for which data is required to be retained, the greater the risk the security of that data may be compromised. In this regard, while the kinds of information identified @187A(2)(a) are required to be retained for longer than 2 years, we note that @187C(2) makes provision for the period specified to be reduced to 2 years from when the information is brought into existence by regulation. Proposed regulation 6 in the draft Amendment Regulation currently identifies 'information of a kind referred to in paragraph (c), (d), (e) or (f) in the column 2 of item 1 of the table in regulation 5' as being required to be retained for the period set out in @187C(1)(b).

---

[23] The PJCIS heard submissions concerning the risks posed by retaining data and what was referred to in the PJCIS' report as the 'honeypot' effect: see the PJCIS Report, Chapter 5 pages 167-175.

Sensitive: Legal

1.62. @187C(3) provides that the time periods for which information is required to be kept are minimum periods and service providers are not prevented from keeping information or a document for a longer period. Service providers that are subject to the Privacy Act must only keep information for longer periods if they need to do so for their own business purposes, otherwise they will be required to destroy the information as required under APP 11.2. Service providers who do not now have a business reason for keeping information beyond the period required by the data retention provisions should establish processes for prompt destruction of personal information after the expiry of the statutory time period.[24]

Access and correction

1.63. APP 12 imposes requirements upon APP entities to permit individuals to access personal information about them which the entity holds in certain circumstances. Similarly, APP 13 imposes requirements on APP entities in defined circumstances to correct personal information they hold. The data retention regime does not contain any provisions relating to access and correction of information, and the provisions of the draft Amendment Bill will not make any changes in relation to this aspect of the handling of personal information by service providers.

CHANGES TO ENFORCEMENT BODY DEFINITIONS AND AUTHORISATION ARRANGEMENTS

1.64. As outlined in paras 1.18-1.20 above, the draft Amendment Bill makes some changes to the types of agencies that will be authorised under the TIA Act to access and use stored communications or telecommunications data. The effect of these changes, and our analysis of the privacy issues and implications raised by these changes, is discussed further below.

Relevant information-handling aspects of current telecommunications law that are not altered by these changes

1.65. As a preliminary point, it is significant to note that these changes do not:

- alter the procedures that are currently in place under Chapter 3 of the TIA Act for agencies to apply for stored communications warrants
- alter the level of authority to access stored communications that is given to agencies when a warrant is issued (see further s 117 of the TIA Act) or the notification requirements applying in these circumstances (see further s 121 of the TIA Act)
- alter the circumstances in which the holders of telecommunications data are authorised to disclose relevant information or documents to an agency on a voluntary basis (see further s 177 of the TIA Act) and use telecommunications

[24] The Australian Information Commissioner's APP Guidelines at paragraph 11.27 stress that an organisation should have practices, procedures and systems in place to identify personal information that needs to be destroyed or de-identified.

Sensitive: Legal

data for purposes associated with that disclosure (see further s 181 of the TIA Act)

- alter the circumstances in which agency officers may authorise access to telecommunications data contained in existing information or documents (see further ss 178, 178A and 179 of the TIA Act) or authorise access to prospective information or documents containing such data (see further s 180 of the TIA Act), or
- alter the operation of the detailed secrecy provisions in Chapter 4 of the TIA Act which create primary and secondary disclosure/use offences in respect of the broader handling of telecommunications data for which an authorisation exists under the TIA Act or the detailed secrecy provisions in ss 276, 277 and 278 of the Telecommunications Act which create primary disclosure/use offences in relation to prescribed information or documents (including information relating to carriage services supplied, or intended to be supplied, to another person by a carrier or carriage service provider or the affairs or personal particulars (including any unlisted telephone number or any address) of another person).

Broader information-handling obligations that are not altered or otherwise affected by these changes

1.66. Related to this, these changes do not otherwise affect, displace or modify the other broader information-handling obligations that apply to the persons and entities which are subject to the specific TIA Act and Telecommunications Act provisions summarised above. These broader information-handling obligations derive from sources such as:

- the Privacy Act (for those criminal law-enforcement agencies / enforcement agencies and holders of telecommunications data comprising 'agencies' and 'organisations' within the meaning of that Act)
- State and Territory privacy laws (for those criminal law-enforcement agencies / enforcement agencies comprising State or Territory agencies)
- detailed secrecy provisions in Commonwealth, State or Territory legislation establishing or otherwise applying to specific criminal law-enforcement agencies / enforcement agencies.[25]

1.67. The various TIA Act and Telecommunications Act provisions outlined briefly above, as well as broader information-handling obligations, are clearly relevant to the ensuring the secure and limited handling of stored communications and telecommunications data, including personal information. As these current arrangements for accessing, using and disclosing relevant information and

[25] In the time available, it has not been possible for us to give detailed consideration to the broad range of laws (and particular secrecy provisions within those laws) that may have some relevant operation in this context. By way of example, however, we mention the potential relevance of provisions such as s 60A of the *Australian Federal Police Act 1979* (Cth), s 127 of the *Australian Securities and Investments Commission Act 2001* (Cth), reg 607 of the *Police Force Regulations 1979* (WA) (made under s 9 of the *Police Force Act 1892* (WA)) and s 54 of the *Independent Commissioner Against Corruption Act 2012* (SA).

documents are not generally affected by the proposed amendments set out in the draft Amendment Bill, our comments in this PIA should be read against the general background of these current arrangements. However, they should not be taken as applying to any matters that go beyond the matters specifically raised by the draft Amendment Bill.

1.68. Following on from this, except to the extent that these current arrangements are directly relevant to the proposed amendments set out in the draft Amendment Bill, we have not analysed the operation of the above TIA Act and Telecommunications Act provisions or other related laws in detail for the purpose of preparing this PIA. Instead, we have assumed that the persons and entities to which the TIA Act, Telecommunications Act or other related laws apply are handling, and will continue to handle, relevant information and documents (including information and documents comprising personal information) consistently with their various legislative obligations.

The narrowing effect of these changes – a privacy positive

1.69. Turning to the specific changes in the draft Amendment Bill relating to enforcement agencies accessing stored communications under warrant and accessing telecommunications data, it seems likely to us that the proposed changes will have 2 significant overall effects. Both of these effects result in these provisions having more limited coverage and application. In light of this, we see the proposed changes as privacy positives.

1.70. The first overall effect is that the total number of agencies that will be able to:

- access stored communications under warrant, or
- rely on an authorisation to access telecommunications data

is likely to be reduced as a result of these amendments.

1.71. Going forward, only 'criminal law-enforcement agencies' as defined will be able to apply under Chapter 3 of the TIA Act to access stored communications under warrant. Under the current law, warrant applications are able to be made by an 'enforcement agency'. This term is more broadly defined and encompasses various types of agencies that will not automatically fall within the new narrower definition of 'criminal law-enforcement agency'. For such an agency to be covered under the new definition, it would be necessary for that agency to make a specific application to the Attorney-General for a declaration that it is a 'criminal law-enforcement agency' for the purpose of these provisions. Unless such a declaration was made in relation to it, the agency would no longer be able to apply for a stored communication warrant.

1.72. Going forward, only authorised officers of 'enforcement agencies' as defined will be able authorise access to telecommunications data relying on the system for authorisations set out in Chapter 4 of the TIA Act. Under the current law, an authorised officer of an 'enforcement agency' can authorise such access. This term is more broadly defined and encompasses various types of agencies that will not automatically fall within the new narrower definition of 'enforcement agency'. Again, for such an agency to be covered under the new definition, it would be necessary for

that agency to make an application for a declaration. Unless such a declaration was made in relation to it, the agency would no longer be able to give an authorisation for access to telecommunications data.

1.73. The second overall effect is that, as a result of the proposed amendments, the TIA Act will more clearly and specifically require privacy considerations to be taken into account as part of the process for the Attorney-General to declare additional agencies as 'criminal law-enforcement agencies' or 'enforcement agencies'. As noted above, the new definitions of 'criminal law-enforcement agency' and 'enforcement agency' each provide for such agencies to include 'an authority or body for which a declaration … is in force' (see new s 110A(1)(m) and new s 176A(1)(b)).

1.74. The proposed amendments relevantly provide that, prior to making any declaration under new s 110A or new s 176A, the Attorney-General must have regard to

> (c) whether the authority or body:
>
> (i) is required to comply with the Australian Privacy Principles; or
>
> (ii) is required to comply with a binding scheme that provides a level of protection of personal information that is comparable to the level provided by the Australian Privacy Principles; or
>
> (iii) has agreed in writing to comply with a scheme providing such a level of protection of personal information, in relation to personal information disclosed to it under Chapter 3 or 4, if the declaration is made ….[26]

We note that such an approach was suggested in the OAIC consultation comments and is reflected in the draft Amendment Bill.

1.75. As a practical matter, it appears likely that this will require any agency seeking a declaration from the Attorney-General to provide detailed information in its application about its status under privacy law and the specific use(s) that will be made of the accessed information or documents by the agency and the manner in which this material will be handled by the agency. We think it would be also relevant in this regard for the Attorney-General to give specific consideration to:

- the extent to which the agency making the application is subject to privacy, confidentiality and / or secrecy obligations in relation to its handling of personal information[27]

---

[26] See new s 110A(4)(c) and new s 176A(4)(c).

[27] A particular issue that may also need to be considered in the context of assessing future applications from certain authorities or bodies is that not all of the States have enacted general privacy legislation. Currently, there is no privacy legislation that applies generally to WA and SA bodies and authorities. This means that it will be particularly important for specific confidentiality and secrecy regimes to be identified in this context. See also footnote 25 above for examples of similar types of provisions that are currently in force under WA and SA legislation (although please note that these examples both apply

Sensitive: Legal

- steps that the agency will take internally to protect the accessed information or documents
- applicable regulatory oversight mechanisms, and the capacity for affected individuals to seek recourse against the agency in the event of the potential mishandling of personal information.

We recommend that any explanatory material prepared by the Department relating to this application process make it clear that detailed supporting material will be required in this regard. Detailed work should also be done on the identification of relevant schemes, and analysis of their operation, for the purposes of assisting the Attorney-General to administer paragraphs (c)(i) and (c)(ii) as described above.

1.76. In addition to the specific reference to privacy obligations in new ss 110A and 176A, as discussed above, these provisions also prescribe some other criteria for consideration by the Attorney-General which are generally reflective of good privacy practice and are consistent with some of the obligations imposed under the APPs. In particular, we note the specific requirements for the Attorney-General to have regard to:

- the specific functions of the authority or body making the application,[28] and
- whether having access to the information or documents that would be facilitated through the making of a declaration and associated authorisations would be 'reasonably likely' to assist the authority or body in performing the relevant specific functions.[29]

1.77. These provisions will operate to require that consideration be given to matters similar to those required to be considered when assessing whether particular acts or practices are APP-compliant. For example, they have an effect similar to APP 3.1 (which requires a demonstrable link to be established between the personal information proposed to be collected and the functions or activities of the entity concerned) and APP 6.1 (which requires that personal information be used and disclosed only for the purpose for which it was collected unless another specific exception applies). In light of these similarities, we consider that these criteria can reasonably be said to have a privacy-enhancing effect. This is also supported by the inclusion of a 'reasonable likelihood' test which will require that objective consideration be given to establishing a demonstrable link between accessing the information or documents in question and achieving the stated objective (for example, assisting in the investigation of serious contraventions).

1.78. Such declarations by the Attorney-General may be made subject to detailed conditions (see new s 110(A)(6) and (7) and s 176A(6) and (7)). This provides a clear mechanism for the Attorney-General to limit the types of enforcement powers that may be exercised lawfully in accordance with the TIA Act by the body or

---

specifically to agencies that will be 'criminal law-enforcement agencies' under the new definition).

28 See new s 110A(4)(a) and s 176A(4)(a).

29 See new s 110A(4)(b) and s 176A(4)(b).

Sensitive: Legal

authority subject to the declaration. Again, we consider that this power to impose conditions can reasonably be said to have a privacy-enhancing effect.

INTRODUCTION OF NEW OVERSIGHT MECHANISMS IN RELATION TO OPERATION OF NEW PART 5-1A AND ACTIVITIES OF ENFORCEMENT AGENCIES

1.79. As outlined in paras 1.21-1.25 above, the draft Amendment Bill introduces various new mechanisms for oversight of:

- the operation of new Part 5-1A
- the activities of criminal law-enforcement agencies and enforcement agencies in relation to stored communications and accessing telecommunications data.

Oversight - operation of new Part 5-1A

1.80. To the extent that the additional oversight mechanisms relating to the operation of new Part 5-1A will contribute to public awareness of the operation and effect of the data retention scheme, then we consider that they will peripherally support good privacy outcomes in that they will provide a further vehicle by which individuals could potentially become aware of the circumstances in which their personal information is collected, held, used and disclosed. However these mechanisms will be additional to, and are no substitution for, meeting specific legal requirements (under the APPs and similar) to notify individuals of these matters.

1.81. We further note that @187P(3) contains a specific privacy protection in requiring the Minister's annual report must not be made in a manner that is likely to enable the identification of a person.

Oversight – activities of agencies

1.82. The oversight role proposed to be given to the Ombudsman under the draft Amendment Act is entirely new. It includes overseeing the activities of enforcement agencies under Chapter 3 of the TIA Act (which, as noted above, is directly relevant to the handling of non content data but is not otherwise being amended under the draft Amendment Act) as well as overseeing the activities of criminal law-enforcement agencies under Chapter 4 of the TIA Act (which, as noted above, is not otherwise being amended under the draft Amendment Act).

1.83. In our view, the amendments relating to the Ombudsman's new role are privacy enhancing in that they will provide a mechanism for identifying both specific instances of non-compliance with TIA Act information-handling obligations (and referring these for action as appropriate) as well as any general agency practices which may create a risk of non-compliance (which can then be ceased or amended as appropriate).

1.84. We note in this context that in the exercise of these additional oversight powers the Ombudsman will necessarily have to collect information that has not previously been required to be collected in the discharge of other functions. In turn, agencies may be obliged to keep further records of information to enable the Ombudsman to discharge these powers. Some of this is likely to be personal information. This

collection of information by the Ombudsman in accordance with the terms of the TIA Act will be a collection that is reasonably necessary for, or directly related to the functions of the Ombudsman and will be consistent with the obligation set out in APP 3.1. As this additional collection of information will be for purposes related to enhancing the level of privacy protection in relation to the operation of Chapters 3 and 4 of the TIA Act, we see it as a privacy positive. Further, to the extent that new ss 151 and 186A may oblige agencies to keep further records of personal information, we do not consider that such obligations would be inconsistent with the requirements set out in APP 11 (or in any equivalent provisions in State or Territory privacy laws or other applicable schemes).

OVERALL EFFECT AND IMPACT OF THESE CHANGES AND RELATED RECOMMENDATIONS

1.85. It can be seen from the above discussion that the proposed changes to the TIA Act set out in the draft Amendment Bill raise various potential privacy issues for consideration.

1.86. In relation to the amendments specifically concerning the retention of non content data, privacy issues are raised in analysing the types of data that will be required to be retained by service providers and the time for which they must be retained, assessing the effect of these changes both for service providers and for individuals who use the regulated services and understanding how these changes interact with existing privacy laws. As noted above, the TIA Act data access scheme as it presently operates has significant implications for personal privacy. Nevertheless, based on the information available to us, we have concluded that the proposed changes set out in the draft Amendment Bill do not appear to have significant privacy implications. Our assessment of these changes against APP obligations and our recommendations below should be noted in this regard.

1.87. In relation to the amendments specifically concerning the changes to enforcement body definitions and authorisation arrangements, privacy issues are raised through consideration of the narrowing effect of these amendments and the operation of the existing privacy regimes and associated obligations that apply to the bodies and authorities that will fall within the new definitions (including by way of specific declaration). Overall, we have concluded that the proposed changes relating to this area are likely to be privacy-enhancing.

1.88. In relation to the amendments specifically concerning the new oversight mechanisms, is necessary to consider privacy issues relating to public reporting mechanisms, the imposition of new record-keeping obligations on enforcement agencies, and the Ombudsman's further powers to access additional information from and report on the activities of enforcement agencies. Overall, we have concluded that the proposed changes relating to this area are likely to be privacy-enhancing.

1.89. We recommend that the Department give further consideration to the following matters:

Sensitive: Legal

- that the period for which specific categories of data is required to be retained continue to be monitored in consultation with enforcement agencies and other relevant stakeholders and that, as needed, consideration be given to whether retention periods may be able to be made shorter for particular types of data
- that any explanatory material prepared by the Department relating to application process for bodies and authorities to apply for a enforcement declaration make it clear that detailed supporting material will be required in this regard
- that detailed work be done on the identification of relevant privacy schemes, and analysis of their operation, for the purposes of assisting the Attorney-General to administer the declaration arrangements.