Appendix 1

Correspondence

ATTORNEY-GENERAL

CANBERRA

MC14/22729

Senator Dean Smith
Chair
Parliamentary Joint Committee on Human Rights
PO Box 6100
Parliament House
CANBERRA ACT 2600

Dear Senator Dean,

Thank you for the 15th report of the Parliamentary Joint Committee on Human Rights to the 44th Parliament, in which the Committee requested further advice in relation to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. I greatly appreciate your Committee's interest in the Bill and support for the Government's objective to increase both public safety and the ability for victims of crime to have recourse to justice.

I have attached detailed responses to the Committee's suggestions. In short, the Government firmly believes that the Bill represents a reasonable, necessary and proportionate limitation on the right to privacy for the protection of national security, public safety and for addressing crime. These measures are critical to protecting the right to life, security of the person and public confidence in communications technology. The scheme will not undermine legal professional privilege in any way.

The Government believes that a two year retention period is appropriate, particularly given the long term nature of many national security and complex criminal investigations and the fact that many victims of crimes, such as sexual assault, do not immediately report their allegations. In this regard, I note that the security and law enforcement agencies have expressed a strong preference for a longer retention period.

In addition, requiring criminal law enforcement agencies to obtain a warrant for every metadata request, or allowing an individual to challenge access to their metadata would be impractical and frustrate law enforcement efforts. Such access restrictions would only serve to adversely affect victims of crime, the very people governments and our law enforcement and security agencies are entrusted to protect. Further, limiting metadata access to investigation of serious crimes, or its use to the purpose for which it was obtained, would be inconsistent with our international obligations, including under the Convention on Cybercrime.

The Government has published the data set proposed to be prescribed by regulation, and has referred the proposed data set to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) alongside the Bill. The Government has also worked with industry through a joint Government-industry working group on possible refinements to the data set, and provided a report to the PJCIS to assist its consideration. The Government looks forward to receiving the PJCIS report, which is due to be tabled on 27 February 2015.

Finally, I have also attached an op-ed by Alastair MacGibbon, Director of the Centre for Internet Safety at the University of Canberra, which addresses a number of the issues covered in your report.

I look forward to continuing to work with you on this important public safety and national security policy. Should you have any questions please do not hesitate to contact my National Security Adviser, Mr Justin Bassi, on (02) 6277 7300.

Yours faithfully

(George Brandis)

Encl:
1. Response to matters raised by the Parliamentary Joint Committee on Human Rights
2. Op-ed, Alastair MacGibbon, Director of the Centre for Internet Safety, University of Canberra

17 FEB 2015

Australian Government response to the 15th report of the Parliamentary Joint Committee on Human Rights to the 44th Parliament
Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) supplements oversight mechanisms which are already in place to ensure privacy and human rights are protected. Existing safeguards will be maintained under the mandatory data retention scheme. For instance, the Privacy Commissioner will continue to assess industry's compliance with the Australian Privacy Principles, and monitor its non-disclosure obligations under the Telecommunications Act. The Inspector General of Intelligence and Security currently inspects and reports on ASIO's access to data.

The Bill protects privacy and human rights by limiting the range of agencies permitted to access telecommunications data and introducing several new oversight mechanisms. They include:

- Agencies to maintain comprehensive records relating to their access, use and disclosure of stored communications and telecommunications data;
- The Commonwealth Ombudsman to inspect access to, and the use of, telecommunications data by Commonwealth, State and Territory enforcement agencies to ensure their compliance with the TIA Act;
- The Attorney-General's Department to include information on the operation of the scheme in its annual report to Parliament.
- The Parliamentary Joint Committee on Intelligence and Security will review the operation of the data retention scheme after 3 years of the scheme's full implementation.

These safeguards are consistent with the bipartisan recommendations from the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its 2013 *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation.*

Proportionality of collecting metadata

The Committee has expressed a view that the proposed data retention arrangements are intrusive of privacy and that this raises an issue of proportionality.

The Australian Government believes that requiring telecommunications providers to retain a limited subset of telecommunications data about all customers is a proportionate response to the threat posed by terrorism, and serious and other crimes such as sexual assault and paedophilia. Case-by-case access to telecommunications data provides the foundational information critical to investigations with the minimum possible intrusion on privacy that is practicable.

Telecommunications data is critical to the investigation of almost any criminal activity, serious or otherwise, where that activity that has been facilitated, enabled or carried out via communications technology. It is essential for investigations into criminal activities and activities prejudicial to security that are conducted exclusively online, such as hacking and cyber-espionage, and activities with a physical manifestation that are further enabled by the internet, such as identity theft and child exploitation. Where an investigation involves an internet-based communication, metadata is often the only investigative lead as such communications leave no physical evidence.

Access to metadata is often the least-privacy intrusive tool available to agencies to undertake the foundational steps in an investigation. It can help build a picture of a how a suspect communicates with criminal associates. Importantly, from a privacy perspective, it allows investigators to identify suspects and exclude others from suspicion and therefore from further, more intrusive, investigation techniques such as telecommunications interception or search warrants. The use of physical surveillance or a surveillance device to identify with whom a suspect has been communicating can result in the collection of the content of communications involving that person, as well as the content of conversations occurring in their vicinity.

The Bill has been drafted to protect individual privacy and human rights while ensuring that data retention remains of practical utility for national security and law enforcement purposes. 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 *Telecommunications (Interception and Access) Act 1979* and the *Australian Security and Intelligence Organisation Act 1979* strictly control the circumstances in which agencies may access, use and disclose telecommunications data and impose criminal penalties for the misuse of such information. This will not change. Additionally, the Bill significantly limits the range of agencies permitted to access telecommunications data and introduces comprehensive independent oversight of all aspects of the access to, and use and disclosure of, telecommunications data by enforcement agencies.

Any privacy implications associated with the increased volume of data which may be generated by the new requirements are mitigated by the obligations imposed by the *Privacy Act 1988*.

The Australian Privacy Principles apply to personal information held by regulated entities. Service providers covered by the Privacy Act must ensure the quality and/or correctness of any personal information and keep personal information secure. The Act imposes obligations regarding the destruction of personal information. The Act also requires regulated service providers to put in place risk-based safeguards against unauthorised access to and misuse of personal information held by industry. The Privacy Commissioner will continue to have oversight of carriers' collection and retention of personal information for regulated service providers.

To the extent that some providers would not be required to comply with the Australian Privacy Principles, retained data would be subject to the same security standards as other data on a service providers' network, including the application of technical and organisational measures to ensure confidentiality, integrity and availability, so that the retained data can only be accessed by authorised personnel. Service providers which are non-APP entities are also subject to data protection obligations under the *Telecommunications Act 1997*.

There are other important safeguards and oversight mechanisms in place. Telecommunications data is protected information. The Telecommunications Act makes it an offence for a service provider and its employees to disclose metadata without consent. Similarly, it is a criminal offence for a police officer or official to use or disclose telecommunications data that has been obtained by their agency, except for one of the limited purposes set out in the Act. ASIO's access to, and use and disclosure of, metadata is subject to oversight by the Inspector-General of Intelligence and Security. Further, the activities of

Federal law enforcement agencies, for example, are subject to Ministerial oversight, scrutiny during Senate Estimates hearings and Parliamentary Committee inquiries and investigations by the Australian Commission for Law Enforcement Integrity. In addition, statistical information on requests for data by law enforcement from telecommunications service providers are reported on annually by the Attorney-General.

The extensive oversight regime contained in the Bill will also empower the Commonwealth Ombudsman to assess agency compliance with their obligations under the *Telecommunications (Interception and Access) Act 1979*. The regime supports effective oversight of agencies by providing precise compliance obligations and more consistent reporting on access to telecommunications data.

The Bill also includes a mechanism for the Communications Access Coordinator to grant an exemption to a service provider from some or all of the mandatory data retention obligations. This exemption mechanism indirectly strengthens the right to privacy by providing a means of reducing data retention obligations, such as where the volume of data to be retained is disproportionate to the interests of law enforcement and national security in that data.

Legislating for mandatory data retention is a necessity. Australia's law enforcement and national security agencies are facing several challenges which have increased their need to reliably access telecommunications data. There has been a long-term decline, and significant industry inconsistency, in the retention of relevant telecommunications data. Without legislative obligations, the Government does not have the ability to address changes in retention practices that significantly degrade agencies' investigative capabilities.

There are no practical alternatives to a data retention scheme that would provide the information agencies need. 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. The purpose of data retention is to introduce a consistent industry standard to ensure that certain limited types of telecommunications data are consistently available.

If the relevant metadata has not been retained, a range of crimes will go unsolved. For example, in a current major child exploitation investigation, the Australian Federal Police (AFP) has been unable to identify 156 out of 463 potential suspects, because certain providers do not retain the necessary Internet Protocol (IP) address allocation records. These records are essential to link criminal activity online back to a real-world person.

For these reasons, the Government believes that a mandatory data retention regime applying to all customers is reasonable, necessary and proportionate.

Regulating the data set

The Committee has expressed concern that the types of data to be retained will be specified by a regulation made pursuant to proposed section 187A(1)(a) in the Bill. The Government believes the combination of primary and delegated legislation is appropriate in this context. However, I acknowledge that several submitters to the current PJCIS inquiry have raised this issue and that the PJCIS is giving further consideration to both the data set and the mechanism through which it should be prescribed. I look forward to that Committee's views and will give further consideration to the range of views expressed in this regard.

Defining 'content'

The Committee has recommended that the Bill be amended to provide a clear definition of 'content' in the primary legislation.

This recommendation would likely result in the opposite of the Committee's desired effect. The Australian Law Reform Commission effectively recognised this risk in its report on Australian Privacy Law and Practice (ALRC Report 108). The report concluded that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) should not exhaustively define what constitutes telecommunications data, in order to allow it to continue to apply in the face of rapid technological change within the telecommunications industry. The merits of technological neutrality in the context of data are equally applicable to defining content. The broad definition in the TIA Act is capable of being interpreted in light of rapid changes in communications technology in a way that an exhaustive, static definition would not.

If the legislation were to include an exhaustive list of that which comprises 'content', it would likely result in the legislation failing to keep pace with rapid changes in the technology offered by the telecommunications industry. Any new types of information that emerge as a result of rapid technological change would fall outside the defined list and would be excluded from the meaning of content.

The TIA Act includes provisions which, when read in conjunction with a broad definition of content, create a strong incentive for telecommunications industry and agencies to take a conservative approach to accessing content. In particular:

- any person who believes that the content or substance of their communications has been unlawfully accessed under a data authorisation can challenge that access and, if successful, to seek remedies under Part 3-7 of the TIA Act
- except for limited exceptions, it is a criminal offence for a service provider to disclose the content or substance of a communication without lawful authority, and
- it is a criminal offence for officials of law enforcement and national security agencies to use or disclose unlawfully accessed stored communications except in strictly limited circumstances.

The TIA Act will continue to maintain a general and effective prohibition on the interception of, and other access to, telecommunications content except in limited circumstances.

Two year retention period

The Government believes a two year retention period is reasonable, necessary and proportionate, and is supported by international evidence and the domestic experience of law enforcement and national security agencies.

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. For telecommunications data, there is an additional risk that business practices will destroy valuable evidence.

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.

Telecommunications data is often used at the early stages of investigations to build a picture of a suspect and their network of associates. Agencies begin their investigations several steps behind perpetrators. The ability to reconstruct events leading up to and surrounding a crime allows agencies to rapidly determine the size and scope of an investigation. Alternative methods, such as physical surveillance, cannot provide essential historical information required in criminal investigations.

Each of the foundational steps in an investigation takes time and delays outside of the control of law enforcement and security agencies are commonly experienced. There may be delays in the matter being brought to the attention of the relevant agency, either by the victim or by another authority that has been conducting a separate investigation. A witness or victim may only come forward after an extended period of time. Alleged offenders may be unwilling to cooperate. Investigators may take time to identify a key piece of evidence. Expert analysis and input may be required, resulting in the investigation being effectively placed on hold for a period of time. Investigative resources can be temporarily diverted to higher priority matters. Consequently, security and law enforcement agencies may not identify the need to access metadata relating to a specific person, service, device or account for an extended period after the commencement of an investigation or after a relevant incident.

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.

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

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

While the review found that approximately 90 per cent 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.

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. It is also 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. Investigations of particularly serious crimes and series of crimes tend to rely on older retained data given the length of time taken to plan and/or commit these offences or series of offences, the need to identify patterns of criminal behaviour and relations between accomplices to a crime, and the need to establish criminal intent. 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
- investigations into 'lone actor' terrorists – in which metadata retained over an extended period of time can point to contact with other extremists, or other involvement with authorities
- counter-espionage investigations into activities which are long-term, strategic, 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.
- 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 serious and the passage of time frequently means that other primary evidence (such as medical or forensic evidence) may no longer be available. 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.
- financial crimes, which are often only detected well after-the-fact, and investigators may take many months to review relevant evidence before they are in a position to identify suspects and/or their associates and request metadata.

'Necessary' for 'serious offences'

The Committee has suggested that the 'reasonably necessary' test be replaced with a 'necessary' test in the context of the Bill, on the basis that it lacks the requisite degree of precision.

Enforcement agencies may only authorise access to specified metadata where access to that specified metadata is 'reasonably necessary' for a legitimate investigation. Service providers are only required, pursuant to subsection 313(3) of the *Telecommunications Act 1997*, to comply with a data authorisation to the extent that it is 'reasonably necessary' for a prescribed purpose. Service providers may refuse requests that do not meet this requirement.

Amending the test for authorising the disclosure of metadata to circumstances where the disclosure is 'necessary' as opposed to 'reasonably necessary' would result in the privacy protections contained in Chapter 4 of the TIA Act diverging from those contained in the *Privacy Act 1988*.

'Reasonably necessary' is the test under Australian privacy law for the collection, use and disclosure of personal and sensitive information. It is an objective test requiring an assessment as to whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. The 'reasonably necessary' test is used throughout the Australian Privacy Principles, including in relation to the collection of personal and sensitive information, and in relation to enforcement-related activities.

By contrast, the 'necessary' test is used only rarely throughout the Privacy Act, in relation to a limited number of permitted general situations – including where it is qualified by the requirement that the entity 'reasonably believes' that the collection, use or disclosure is 'necessary' - permitted health situations, and certain contractual situations. The Privacy Commissioner has confirmed that the usage of the 'necessary' test as opposed to the 'reasonably necessary' test is explained by the context in which the test is used.

There is no suggestion that the 'necessary' test is more certain, narrow or strict than the 'reasonably necessary' test. By contrast, the High Court has observed 'that there is, in Australia, a long history of judicial and legislative use of the term "necessary", not as meaning essential or indispensable, but as meaning reasonably appropriate and adapted'.[1] The Australian Law Reform Commission has observed, in the context of the former National Privacy Principles, that the term 'necessary' *implies* an objective test.[2]

The replacement of the 'necessary' test from the National Privacy Principles with the 'reasonably necessary' test in the Australian Privacy Principles requires the collection of personal information to be justifiable on objective grounds, rather than on the subjective views of the entity itself and is intended to expressly clarify that the test is objective (rather than implied) and to enhance privacy protection. For the same reasons, it is preferable that access to telecommunications data be based on the 'reasonably necessary' test.

Likewise, the Government does not agree with the Committee's recommendation that access to and use of metadata should be limited to certain categories of serious crimes. The Government believes that it is preferable to restrict access by specifying the agencies that are empowered to authorise the disclosure of data, rather than raise the access threshold to an arbitrarily imposed 'serious crime' threshold. Accordingly, Schedules 2 and 3 introduce provisions to reduce the range of agencies that may access telecommunications data, replacing the general descriptors of the types of agencies that may do so.

In addition, Australia is required to make metadata available for all criminal investigations by virtue of being a party to the Convention on Cybercrime. Article 14 of that Convention requires that Australia and other States parties establish powers and procedures, including

---

[1] *Mulholland v Australian Electoral Commission* (2004) 220 CLR 181, [39].
[2] Ibid, 21.75.

access to historical telecommunications data, to enable the collection of evidence in electronic form of a criminal offence.

Telecommunications data is valuable to combatting all crimes, is less intrusive than other investigative techniques, and should not be arbitrarily limited to a narrow selection of crimes.

Using metadata for a secondary purpose

The Government does not agree with the Committee's recommendation that retained metadata be used only by the requesting agency for the purpose for which the request was made and for a defined period of time. It would unduly and unnecessarily frustrate legitimate law enforcement efforts.

Agencies are often required to conduct joint investigations when a matter spans multiple jurisdictions, when a suspect crosses a border during an investigation. Sometimes the nature and focus of an investigation changes based on new information, requiring information obtained for one purpose to be used for one or more separate purposes. For example, missing person investigations can often become kidnapping, serious sexual assault and/or murder investigations. Security intelligence investigations can transition into criminal investigations and vice versa, particularly in the case of counter-terrorism and counter-espionage.

In addition, agencies conducting an investigation may identify information pointing to additional criminal conduct. For example, agencies investigating organised criminal activity may identify information pointing to corruption or money laundering. Agencies investigating a particular crime may obtain evidence linking the suspect with other, unsolved crimes. Investigators may often uncover evidence that is directly relevant to another investigation (such as data demonstrating that a suspect in both investigations is using a covert phone).

There is no basis in international law for the proposition that information gathered by a law enforcement or security agency may be used only for the purpose for which it was obtained. Conversely the need to share such information is directly reflected in the *Convention on Cybercrime*, under which agencies may also be required to respond to a request for mutual legal assistance.

Existing safeguards will continue to apply to access to telecommunications data. A limited number of approved management-level officials in Australian enforcement agencies may authorise the disclosure of specified telecommunications data that is reasonably necessary for a prescribed purpose, and only after having regard to whether any interference with the privacy of any person or persons would be justified, having regard to the likely usefulness of the information and the purpose for which it is sought.

Under section 182 of the *Telecommunications (Interception and Access) Act 1979*, a person may only use or disclose telecommunications data lawfully obtained by an enforcement agency if the use or disclosure is 'reasonably necessary' for the performance by ASIO of its functions, for the enforcement of the criminal law, for the enforcement of a law imposing a pecuniary penalty, or for the protection of the public revenue. The interpretation of 'reasonable necessity' in this context will be similar to its interpretation in relation to the authorisation of the disclosure of data—where the use or disclosure of the specified data would have a demonstrable benefit or assist in enforcing the criminal law, without which there would be a likelihood that such enforcement could not occur. The use of metadata for a prurient purpose, or even as part of an investigation where its use or disclosure is not reasonably necessary for a prescribed purpose, would constitute a criminal offence.

In addition:

- section 182 of the TIA Act makes it a criminal offence, punishable by imprisonment for 2 years, to use or disclose metadata that has been lawfully obtained by an enforcement agency under Divisions 4 or 4A of Chapter 4 of the TIA Act
- section 185 of the TIA Act requires enforcement agencies to retain authorisations made under Chapter 4 of the TIA Act for 3 years. The Bill preserves this requirement, and also introduces comprehensive new record-keeping requirements around access to, and the use and disclosure of metadata by enforcement agencies.
- section 18A of the ASIO Act makes it a criminal offence, punishable by imprisonment for 3 years, to deal in information lawfully obtained by ASIO in connection with its functions, including telecommunications data obtained by ASIO under Division 3 of Chapter 4 of the TIA Act.
- section 18 of the ASIO Act makes it a criminal offence, punishable by imprisonment for 10 years, to communicate such information, subject to a limited number of exceptions to allow for the lawful use and disclosure of lawfully accessed data, and other information in the case of ASIO.

Australian Privacy Principle 11 also requires Commonwealth law enforcement agencies to take such steps as are reasonable in the circumstances to protect personal information in their possession from misuse, interference and loss, and from unauthorised access, modification or disclosure.

The Australian Privacy Principles do not apply to ASIO. However, the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* require the Director-General of Security to ensure that all personal information collected or held by ASIO is protected by reasonable security measures against loss and unauthorised access, use or modification. The use and communication of telecommunications data by ASIO is similarly subject to strict controls under the ASIO Act and the Attorney-General's Guidelines.

The Australian Government's Protective Security Policy Framework also requires agencies to appropriately classify, secure and restrict access to information, including metadata and other information lawfully obtained in the course of an investigation. The need-to-know principle is enshrined within the Framework as are the requirements for officials to hold appropriate security clearances and briefings before they are permitted to receive, use and disclose information. The existence of similar appropriate processes and procedures to give effect to such obligations would be a relevant consideration for the Attorney-General when considering an application for an agency to be declared a criminal law-enforcement agency or an enforcement agency, pursuant to paragraphs 110A(4)(d) and 176A(4)(d), respectively.

The Committee has specifically referenced the statutory ability of ASIO to share information with the Australian Secret Intelligence Service. ASIS's functions and activities include supporting Australian soldiers in combat operations, enabling the safe rescue of kidnapped civilians, counter-terrorism and counter-proliferation. A limit on ASIO's ability to share that information would frustrate those important objectives. The prevention and suppression of terrorism is of great public importance, and the proliferation of nuclear, chemical and biological weapons, as well as their means of delivery, constitutes a threat to international peace and security within the meaning of Chapter VII of the United Nations Charter. I also note that the Committee has, in a more recent report, contemplated that the sharing of information (not limited to metadata) by ASIS with the Australian Defence Force could be necessary and proportionate.

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. 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, including legal advice.

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 *Telecommunications (Interception and Access) Act 1979* 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.

Requiring a warrant

The Government does not agree with the Committee's suggestion that agencies should be required to obtain a warrant to access metadata. It follows that the Government believes that it is unnecessary to have an advocate to ensure impartial assessment of the content and sufficiency of warrant applications to access metadata.

To require a warrant to access metadata would be impractical, and result in a significant degradation in agencies' ability to protect public safety. It would considerably delay agencies commencing almost every counter-terrorism, counter-espionage, organised crime, cyber-security, murder, child exploitation and serious sexual assault investigation, with a considerable risk that critical evidence would be lost. Warrant applications take considerable time to develop, which necessarily delays investigations and creates a risk that perishable physical, electronic and testimonial evidence will be lost.

While metadata is used at all stages of law enforcement and national security investigations, it is predominantly used in the early stages to provide foundational information. By

comparison, the other powers contained in the TIA Act, and virtually all other powers that are subject to a warrant, are used in the latter stages of an investigation. Access to metadata commonly provides the basis for more intrusive forms of investigation, including telecommunications interceptions, search warrants and the use of surveillance devices. It ensures that investigators can exclude others from suspicion and in turn from these investigative techniques. There is a clear distinction that can be drawn between the level of privacy impact occasioned by access to metadata and telecommunications interception or the execution of a search warrant.

In reaching its recommendations about warrants, the Committee has referenced the recent decision of the Court of Justice of the European Union in the *Digital Rights Ireland* case. In finding that the EU Data Directive was not human rights compatible, the Court found that access to data ought to have been dependent upon prior review by a court or independent administrative body.

By contrast, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has expressed a contrary view. The Special Rapporteur has distinguished between the 'surveillance of communications', which 'must only occur… under the supervision of an independent judicial authority' and the 'provision of communications data by the private sector to States' which must be 'sufficiently regulated to ensure that individuals' human rights are prioritized at all times' and 'should be monitored by an independent authority, such as a court or oversight mechanism'.

The requirement to obtain a warrant prior to exercising certain investigative powers is typically reserved for powers that immediately and irretrievably engage the essence of a particular fundamental right or freedom. Conversely, the exercise of powers that do not engage the essence of fundamental rights and freedoms, or that only create a potential for future engagement of those rights and freedoms should the agency take subsequent, follow-up action, are typically not subject to a requirement for independent authorisation by a judicial or quasi-judicial officer. In those circumstances, the preferable approach is to ensure that appropriate controls and safeguards are implemented at relevant points of the information cycle and, in particular, around how agencies may use data.

The use of data under the TIA Act is strictly controlled. Agencies may only access metadata on a case-by-case basis and, in the case of enforcement agencies, only where and to the extent that access is reasonably necessary for a prescribed purpose, such as the enforcement of the criminal law. Access may only be approved by management-level officials, who are required to have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the likely relevance and usefulness of the information or documents, and the reason why the disclosure or use concerned is proposed to be authorised. ASIO may only access metadata in connection with its functions and in accordance with the Attorney-General's Guidelines. The unauthorised use of metadata is a criminal offence punishable by two years' imprisonment, in the case of an enforcement agency, or three years' imprisonment, in the case of ASIO.

In addition, section 276 of the *Telecommunications Act 1997* makes it an offence for a carrier, carriage service provider or their employees to disclose the affairs or personal particulars of any other person that has come in to their knowledge or possession. A contravention of that offence is punishable by a term of imprisonment of up to 2 years.

Similarly, the *Privacy Act 1988* may apply to some information required to be retained by virtue of the Bill. That Act provides effective civil remedies for persons whose privacy may have been breached. Part V of that Act includes a comprehensive scheme for the making of,

and investigation of complaints. The Privacy Commissioner also has the power to make determinations in relation to breaches of the Australian Privacy Principles.

In addition to the accountability mechanisms earlier outlined, the Bill introduces additional safeguards. In particular, the Bill will significantly limit the range of agencies permitted to access metadata, and will introduce comprehensive, independent oversight by the Commonwealth Ombudsman for all Commonwealth, state and territory agencies accessing metadata. This oversight function will support accountability and enable assessment of an agency's overall compliance with their powers to access and use stored communications and telecommunications data.

The Ombudsman will 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 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.

The Bill also 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 including 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 Bill also 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.

Prior notification and challenge

The Committee's suggestion that individuals be notified when their telecommunications data is subject to an application for authorisation for access, or once it has been accessed, and be then able to challenge such access, would hamper investigations. The covert investigative powers contained in the *Telecommunications (Interception and Access) Act 1979* and *Surveillance Devices Act 2004* are generally used where the integrity of an investigation would be compromised by revealing its existence. In circumstances where overt access to metadata and other communications-related information is possible, such as where an agency is seeking information from a living victim of a crime, agencies are generally able to obtain that information from a provider with the person's consent.

theage.com.au
THE AGE

Access to metadata is vital for crime fighting: says internet safety advocate

Alastair MacGibbon
Published: January 30, 2015 - 4:33PM

- Privacy Commissioner questions two-year plan: inquiry

In my career I have witnessed the challenge of fighting crime while attempting to balance individual privacy with what can be deemed a reasonable level of intrusion.

It is a challenge the government is currently facing, but sadly, there are plenty of myths that need to be debunked for us to have a rational discussion about "metadata". It's a word most people didn't know until recently, and one which even governments have had difficulty defining.

What is metadata?

Metadata can be defined very broadly or very narrowly. Essentially it refers to information generated as a result of an electronic communication, such as the identity of a person who subscribes to a telephone service and a record of the numbers they have dialled.

The government is intentionally narrow in its definition of metadata: it is seeking things such as phone call records and our dynamically-allocated IP addresses be retained. On any day, several people may be allocated the same IP address, so it is critical to protect the rights of innocent people by ensuring the right user is tied to the offence. To emphasise the point, metadata is not only incriminatory, but exculpatory as well, meaning that having a system in place that can properly collect and assess this data serves everyone's interests.

A new power?

No. For many years, police across Australia have used metadata, without fanfare or warrant, to investigate serious crimes such as terrorism, drug trafficking, child exploitation and murder. Offenders have been caught. Victims of crime have been afforded some sense of justice and the public has been protected.

With developments in information and communications technology, however, this type of data is less routinely kept by service providers for billing purposes and, accordingly, situations arise where, without regulation, it may be lost as a vital resource for investigators. I saw this trend starting back in the early 2000s when I set up the Australian High Tech Crime Centre – and the fragmentation and inconsistencies have only increased.

In recent years, AFP Commissioners and their state and territory counterparts have consistently highlighted the issue of metadata retention as one of the most important issues affecting law enforcement. The government's bill, if passed, will require communication providers to keep this metadata for two years to ensure its availability, if needed, as part of a criminal investigation. This follows around 25 western countries who have implemented data retention laws.

Search warrants

Interestingly, even those who oppose the bill largely agree that metadata is a vital investigative tool that has helped solve many serious crimes. The trouble is that they propose a regime of search warrants to access it which will, for all intents and purposes, destroy its utility.

Forcing police to obtain a search warrant or court order to access metadata will not only see investigations significantly and unnecessarily delayed but also risk grinding the courts to a halt under the sheer weight of applications. The threshold for warrants is justifiably high: for police to enter our premises or vehicle and search

and seize items it should be – it is a major impost on privacy. Accessing our telephone records, while clearly privacy infringing, simply isn't in the same league and shouldn't have the same high benchmark for access.

While access to metadata is currently obtained without a warrant, it isn't without authority. Commissioned officers must sign data access requests, and the authority for such requests is enshrined in legislation. Importantly, the proposed reforms introduce an oversight regime, which includes the Commonwealth Ombudsman, the Privacy Commissioner and the Inspector General of Intelligence and Security (IGIS). The reforms also contain a number of safeguards that significantly reduce and limit the range of agencies permitted to access telecommunications data.

Content of communications

Some have argued that if you piece enough metadata together, ranging from location information to lists of people communicated with, it is the same as knowing what was said between those people. This is flawed. Knowing I've met with someone and where I've gone is not nearly as rich as actually knowing what I've said to that person. It's been explicitly and consistently said that content information – including information about websites I have visited – is excluded from the proposed reforms.

Cost

Some telcos have argued it will cost massive sums of money to configure their systems to capture and store this data. All government regulation costs money. From recordkeeping for tax purposes through to pharmaceutical companies having drugs on the market, costs are built into systems. Every business – and household – knows that the cost of electronic storage has dropped dramatically in recent years.

Privacy

As a society we accept that police agencies wield enormous power which includes the power to use lethal force and to enter and search our premises.

Interestingly, those most aggrieved by the proposed legislation have not been up in arms about the amount of data captured, traded, sold and exploited by private companies. While the chances of any of us having our data lawfully accessed by the government remains rare, our data is used every day without our knowledge by private companies.

A way ahead?

Balancing police powers against privacy is difficult to achieve and like many things in life, will polarise the community. For this reason, independent oversight and appropriate checks and balances are a critical part of ensuring that the confidence and support of the broader community is maintained.

The challenge Australia now faces is whether to condemn our law enforcement agencies to losing a valuable source of critical crime-solving information, as the quality of metadata held by telecommunication companies continues to erode; whether to hamstring these agencies by raising the bar for access too high; or, whether to keep the metadata regime in step with technology changes so that it can be used by the agencies within a framework of oversight and control on access and use.

Alastair MacGibbon is director of the Centre for Internet Safety at the University of Canberra and general manager, security business, at Dimension Data Australia.

SENATOR THE HON. ERIC ABETZ
LEADER OF THE GOVERNMENT IN THE SENATE
MINISTER FOR EMPLOYMENT
MINISTER ASSISTING THE PRIME MINISTER FOR THE PUBLIC SERVICE
LIBERAL SENATOR FOR TASMANIA

Senator Dean Smith
Chairman
Parliamentary Joint Committee on Human Rights
Parliament House
CANBERRA ACT 2600

19 NOV 2014

Dear Senator

I refer to your further letter of 28 October 2014, concerning the Parliamentary Joint Committee on Human Rights' review of the Commonwealth Cleaning Services Repeal Instrument 2014.

The Committee's assertion that the repeal of the Commonwealth Cleaning Services Guidelines may breach Australia's Human Rights obligations is unfounded as is the assertion that revoking the Guidelines disproportionately impacts workers based on their racial background. The latter allegation is, to be frank, repugnant. I firmly repudiate any such claims. Not even the unions make such a bizarre and offensive assertion.

I again re-iterate that the Cleaning Services Guidelines were a small scale Government procurement policy that would have applied to less than one per cent of the cleaning workforce. It is not the role of the Australian Government to impose policies over and above the safety net provided through the established workplace relations framework. In particular, it is not this Government's policy to permit special wage fixing deals for highly unionised industries, to misuse the Government's procurement rules to serve union interests, or to circumvent the role of the Fair Work Commission.

The Guidelines were flawed and applied to less than one percent of the entire cleaning industry. The Guidelines mandated that employers hand out union membership material and forced them to pay their workers well above award wages, without any requirement to demonstrate genuine productivity gains. The Committee's repeated views avoid engaging with and appears difficult to reconcile with my earlier advice that the Guidelines had no impact whatsoever on the more than 99 percent of workers in the industry that don't work in Government offices located in central business district locations. These matters do not give rise to human rights issues. Wage setting in Australia, is and has been for many years, the responsibility of the Fair Work Commission and not the Government of the day. The previous government's decision to issue the Guidelines, to give special arrangements to a tiny subset of workers in the industry, in cooperation with a particular union, undermined that role. The Cleaning Services Award 2010 sets minimum wages and conditions for all cleaners in Australia and, beyond this, higher wages and conditions should rightly be negotiated via enterprise bargaining. To assert otherwise and then suggest racial discrimination has the logical (but I am sure unintended) consequence of accusing the Fair Work Commission of such behaviour.

The existing enterprise bargaining system meant that many cleaners (through at least 65 Government cleaning contracts) were remunerated at the higher levels before the Guidelines commenced in 2012. Agencies continue to have the flexibility to engage cleaning companies that pay above award wage and conditions. Since the revocation of the Guidelines, that is still occurring.

CANBERRA: MG 68, Parliament House, Canberra ACT 2600. Phone: 02 6277 7320 Fax: 02 6273 4115
HOBART: 136 Davey Street, Hobart TAS 7001 Phone: 03 6224 3707 Fax: 03 6224 3709
minister@employment.gov.au http://abetz.com.au

Our Ref BR14-003602

This exercise would indicate the Committee has seriously lost its way by attempting to conflate matters of government procurement, and the payment of wages above relevant minimum standards, with issues of human rights. Such an approach, if I may say, does not appear to be the most effective use of the Committee's time and serves only to discredit the more serious and worthy issues of human rights.

I trust the matter will rest.

Yours sincerely

ERIC ABETZ

The Hon Scott Morrison MP
Minister for Immigration and Border Protection

Senator Dean Smith
Chair
Parliamentary Joint Standing Committee on Human Rights
S1.111
Parliament House
CANBERRA ACT 2600

Dear Senator

Response to questions received from Parliamentary Joint Committee on Human Rights

Thank you for your letters of 23 September 2014 in which further information was requested on the following bill and legislative instruments:

- *Migration Amendment (Protection and Other Measures) Bill 2014*
- *Migration Amendment (Repeal of Certain Visa Classes) Regulation 2014 [F2014L00622]*
- *Migration Legislation Amendment (2014 Measures No. 1) Regulation 2014 [F2014L00726]*

My response to your requests is attached.

I trust the information provided is helpful.

Yours sincerely

The Hon Scott Morrison MP
Minister for Immigration and Border Protection
21 / 10 /2014

1.150. The committee therefore requests the further advice of the minister as to the particulars of any safeguards or policies in place to ensure women and persons with disabilities are not disadvantaged by proposed section 5AAA

I note that the committee 'remains concerned, based on the information provided, that proposed section 5AAA of the *Migration Act 1958* (the Act) may lead to indirect discrimination against women and persons with a disability'.

As previously discussed, proposed section 5AAA explicitly states an existing responsibility of people who seek protection in Australia, consistent with the UNHCR Handbook. It does not introduce a new responsibility.

Section 5AAA does not change the decision-maker's obligations regarding the assessment of claims for protection. The duty to evaluate and ascertain all relevant facts is shared between the applicant and the decision-maker, consistent with UNHCR guidelines. Decision-makers may continue to ask questions, seek clarification and check that a person's claims are consistent with generally known facts and the specific country situation in question. Decision-makers must act in good faith to fully assess Protection visa applications and afford procedural fairness to asylum seekers in accordance with the Codes of Procedure in the Act.

Current policy guidance already provides safeguards from indirect discrimination to applicants who are women or people with a disability. This policy guidance is publicly available, will continue to apply, and will be updated to appropriately reflect the new section 5AAA.

The departmental "Gender Guidelines" comprehensively detail particular considerations to address potential barriers affecting female applicants. The guidelines recognise women and girls may experience particular acts of persecution and discrimination, and they address how gender related persecution can affect an applicant's ability to present their claims, lodgement of an application, interview management and confidentiality. The "Gender Guidelines" are consistent with and make direct reference to gender guidelines provided by the UNHCR, including the 2008 UNHCR "Handbook for the Protection of Women and Girls".

Detailed policy guidelines are provided in the "Protection Visa Procedures Advice Manual", the "Refugee Law Guidelines" and the "Complementary Protection Guidelines" regarding claims on behalf of survivors of torture and trauma. These guidelines comprehensively address the needs of applicants with disabilities that have resulted from torture or trauma, and include advice regarding the conduct of interviews and the assessment of credibility.

In addition to departmental policy guidelines, the Refugee Review Tribunal (RRT) provides policy guidance to its members that safeguards applicants who are women or people with a

disability from indirect discrimination, namely the RRT "Gender Guidelines" and "Guidance on Vulnerable Persons". Both documents are publicly available on the RRT website: http://www.mrt-rrt.gov.au/Conduct-of-reviews/Legislation-policies-and-guidelines.aspx

Furthermore, primary application assistance is available to protection visa applicants who have arrived lawfully and are disadvantaged or face financial hardship (through the Immigration Advice and Application Assistance Scheme (IAAAS)), and a new Primary Application Information Service (PAIS) will provide application assistance from registered migration agents during primary processing for a small number of illegal maritime arrivals (IMAs) and unauthorised air arrivals (UAAs), who are considered to be the most vulnerable. The departmental tender for PAIS closed on 23 September 2014.

The combination of training, departmental and RRT guidelines and application assistance in certain circumstances mitigates any risk that the proposed section 5AAA will lead to discrimination against women or people with a disability.

1.154. The Committee therefore requests the Minister for Immigration and Border Protection's advice as to whether there are measures or safeguards in place to ensure that section 423A does not have a disproportionate or negative impact on persons with a disability

As discussed above, decision-makers are obliged to act in good faith to fully assess Protection visa applications and afford procedural fairness to asylum seekers in accordance with the Codes of Procedure in the Act. RRT decision-makers must not act in a manner which is inconsistent with departmental policy guidelines for decision-makers and comprehensive policy guidelines are available regarding protection visa applications from survivors of torture and trauma, who may be living with a disability.

The RRT provides specific policy guidance to its decision-makers regarding persons with a disability, namely "Guidance on Vulnerable Persons". The RRT also explicitly advises Tribunal members to be mindful of whether an applicant is living with an illness or disorder that may affect the applicant's ability to give evidence and recall specific events or details in the policy document "Guidance on the Assessment of Credibility".

Under the proposed section 423A, the Tribunal member will draw an inference unfavourable to new claims or evidence if the member is satisfied the applicant does not have a reasonable explanation for not providing the information at the primary stage. A "reasonable explanation" is not defined in the provision as the general principles of administrative law and reasonable decision-making apply. A "reasonable explanation" is one that satisfies a Tribunal member that the new claims and evidence could not be presented earlier because the applicant was unable to do so. A "reasonable explanation" may therefore include a situation where the applicant has a restricted ability to effectively participate in the protection process due to a disability.

The proposed 423AA will be inserted into the Part 7, Division 3 of the Act which deals with 'Exercise of the Refugee Review Tribunal's powers'. The RRT is a statutory body and exists to provide an independent and final merits review of decisions that is fair, just, economical, informal and quick. Tribunal members and staff are aware of the importance of treating those with who they deal with courtesy, respect and dignity.

These important safeguards of fairness and justice are enshrined in legislation. Section 420 of the Act details the RRT's way of operating when it states:

(1) The Tribunal, in carrying out its functions under this Act, is to pursue the objective of providing a mechanism of review that is fair, just, economical, informal and quick.
(2) The Tribunal, in reviewing a decision:

(a) is not bound by technicalities, legal forms or rules of evidence; and

(b) must act according to substantial justice and the merits of the case

I am of the view that such a way of operating is appropriate and conducive to section 423AA not having a disproportionate or negative impact on persons with a disability. Further to this, the Tribunal's procedures are relatively informal, I am not represented and the member will guide the proceedings to suit the circumstances of the case. These procedures are also legislated in Part 7, Division 4 of the Act which I consider to be an important safeguard.

I also refer you to the following webpage which details support organisations - http://www.mrt-rrt.gov.au/Apply-for-review/Support-and-advice/Support-organisations.aspx. Many of these services are funded by the Australian Government.