Australian Government

Attorney-General's Department

National Security
Law and Policy Division

13/9768

31 July 2013

Mr Tim Bryant
Acting Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Acting Committee Secretary

Inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013

Please find attached a submission from the Attorney-General's Department in relation to the Senate Standing Committee on Legal and Constitutional Affair's Inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013.

The Department has consulted with the following portfolio agencies: Australian Commission for Law Enforcement Integrity (ACLEI), Australian Crime Commission (ACC), Australian Customs and Border Protection Service (Customs), Australian Federal Police (AFP) and the Australian Security Intelligence Organisation (ASIO), which all support this submission.

Yours sincerely

Geoff McDonald
First Assistant Secretary
National Security Law and Policy Division

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',[1] which is a significantly narrower range of enforcement agencies.

[1] 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

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.

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.

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]

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.

[THIS PAGE LEFT INTENTIONALLY BLANK]

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.