Australian Government
Department of Home Affairs

An overview of the framework governing access to, and the retention of, telecommunications data

The Parliamentary Joint Committee on Intelligence and Security's review of the mandatory data retention regime

[redacted]

[redacted]

Access to telecommunications data, and the data retention obligations under the *Telecommunications (Interception and Access) Act 1979*[1]

Sections 276, 277 and 278 of the *Telecommunications Act 1997* (Cth) (Telecommunications Act) establish general prohibitions on carriers and carriage service providers disclosing certain information or documents, including telecommunications data.

Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) provides a framework to allow the Australian Security Intelligence Organisation (ASIO) or an *enforcement agency*[2] to lawfully access, disclose and use telecommunications data without breaching the Telecommunications Act.

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (Data Retention Act) introduced a framework at Part 5-1A in the TIA Act to govern the retention of a prescribed set of telecommunications data for two years by communications service providers of relevant services (see section 187A(1) and (3)).

What is telecommunications data?

Telecommunications data is information about a communication, but does not include the content or substance of the communication.[3] Telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony. If an agency wishes to covertly obtain telecommunications data under the TIA Act, they are required to do so under an authorisation in accordance with the provisions in Chapter 4 of the TIA Act.

If an agency wishes to covertly obtain the content of a communication – as opposed to telecommunications data – the agency is required to obtain a warrant in accordance with the provisions in Chapters 2 or 3 of the TIA Act, which regulate telecommunications interception and access to stored communications respectively.

The obligation to retain and protect telecommunications data

The data retention obligations at Part 5-1A of the TIA Act support agencies' pre-existing and longstanding power to access telecommunications data, by ensuring this data is consistently available when it is required for investigations and operations conducted by ASIO and *enforcement agencies*.[4] The introduction of the retention obligations was accompanied by a series of safeguards and oversight arrangements to protect the privacy of Australians and to prevent any unlawful or unauthorised access to telecommunications data. Only ASIO and *enforcement agencies* have access to the subset of telecommunications data that a provider retains for no other reason than to meet their obligations under the data retention regime.

Providers required to retain telecommunications data under the data retention regime

Section 187A of the TIA Act stipulates that the data retention obligations apply to communications services operated by carriers, carriage service providers and internet service providers. This captures providers that own or operate infrastructure (such as servers, routers and/or cables) within Australia that enables one or more of their communications services.

Section 187B of the TIA Act provides an exemption from the data retention obligations for service providers who provide services only to a person's 'immediate circle' such as internet and intranet services provided within corporate

[1] Refer to **Attachment A** for an overview of the regime governing domestic access to, and retention of, telecommunications data under *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act).
[2] *Enforcement agency* is defined in section 176A of the TIA Act. **Attachment B** provides a list of *enforcement agencies*.
[3] Section 172 of the TIA Act makes it clear that telecommunications data does not include the content or substance of a communication.
[4] Agencies have had a longstanding ability to access telecommunications through various Commonwealth legislation. Notably, and more recently, agencies had the ability to access telecommunications data through the then sections 282 and 283 of the Telecommunications Act since 1 July 1997. The *Telecommunications (Interception and Access) Amendment Act 2007* transferred these provisions to the TIA Act to implement recommendations from the 'Report on the Review of the Regulation of Access to Communications by Anthony Blunn AO.'

[redacted]

and university networks. This reflects an assessment that the benefits to agencies of imposing data retention obligations on these networks is outweighed by the privacy and compliance burden.

Further, section 187K of the TIA Act provides that the Communications Access Coordinator may exempt a service provider from any or all aspects of their data retention obligations after having regard for such matters as the interests of law enforcement and national security, and the costs of compliance. Under current administrative arrangements, the Office of the Communications Access Coordinator sits in the Department of Home Affairs.

Telecommunications data to be retained under the data retention regime

Section 187AA of the TIA Act lists the types of telecommunications data that service providers must retain in order to comply with their data retention obligations. To minimise the burden on industry and any perceived privacy intrusion, the TIA Act only requires the retention of telecommunications data that is critical to initiating or furthering investigations and operations. This means that not all so-called 'metadata' is required to be retained.

The datasets to be retained are:[5]

- The subscriber of, the accounts, services, telecommunications devices and other relevant services relating to, the relevant service
- The source of a communication
- The destination of a communication
- The date, time and duration of a communication, or of its connection to a relevant service
- The type of a communication or of a relevant service used in connection with a communication
- The location of equipment, or a line, used in connection with a communication

The above list of datasets must be retained by service providers for two years in accordance with section 187C of the TIA Act.[6]

Section 187A(4) of the TIA Act puts beyond doubt that service providers are not required to keep information about the contents or substance of a communication, a subscriber's web browsing history or communications that pass 'over the top' of the underlying service they provide.

Requirements to protect retained telecommunications data

Section 187LA of the TIA Act provides that the *Privacy Act 1988* (Cth) (the Privacy Act) and the Australian Privacy Principles (APPs) apply in relation to a service provider (as though they were an *organisation* under subsection 6C(1) of the Privacy Act) to the extent that their activities relate to retained data. This section also clarifies that retained telecommunications data in relation to the individual, or a communication to which the individual is a party is 'personal information' which, amongst other things, entitles the individual to access the data in accordance with APP 12.

Section 187BA of the TIA Act requires service providers to protect the confidentiality of retained data by encrypting the information and protecting it from unauthorised interference and access. Service providers are also subject to further obligations to protect information under the Telecommunications Consumer Protection Code and the Telecommunications Sector Security Reforms (contained in Part 14 of the Telecommunications Act).

[5] For a detailed explanation of each dataset, refer to the Home Affairs portfolio submission (Submission 21) to the 'review of the mandatory data retention regime' pg. 11-13; and the explanatory memorandum to the Data Retention Act pg. 46-50.
[6] Section 187C implements recommendation 9 in the 'Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.'

[redacted]

Agencies eligible to access telecommunications data under the TIA Act

The Data Retention Act introduced a new definition of *enforcement agency* to limit the range of agencies that are able to access telecommunications data under the TIA Act, including data retained because of the data retention regime.[7]

The ability to internally authorise access to telecommunications data under the TIA Act – including mandatorily retained data – is reserved for ASIO and the 20 agencies that satisfy the definition of *enforcement agency* in section 176A(1) of the TIA Act.[8] Each of the following are *enforcement agencies*:

- *criminal law-enforcement agencies* as defined at subsection 110A(1) of the TIA Act. These agencies also have the ability to apply for warrants to access stored communications, and
- authorities or bodies declared by the Minister for Home Affairs to be an *enforcement agency* as provided for by paragraph 176A(3)(a) of the TIA Act.

At this time, the Minister for Home Affairs has not declared any authority or body as an *enforcement agency.* Accordingly, the 20 agencies that are *enforcement agencies* are also *criminal law-enforcement agencies.*

Thresholds for access to telecommunications data under the TIA Act

The TIA Act distinguishes between access to historical telecommunications data (data that is already in existence at the time of the request) and prospective data (data that comes into existence during the period the authorisation is in force, and is collected as it is created and forwarded to the agency in near real time).

Historical telecommunications data

An *authorised officer*[9] of an *enforcement agency* is permitted to authorise the disclosure of historical telecommunications data (including data retained because of the data retention regime) if satisfied it is reasonably necessary for:

- enforcing the criminal law (section 178 of the TIA Act),
- enforcing a law imposing a pecuniary penalty or protecting the public revenue (section 179 of the TIA Act), or
- locating a missing person (section 178A of the TIA Act).[10]

Prospective telecommunications data

Section 180 of the TIA Act stipulates that the disclosure of prospective telecommunications data can only be authorised by an *authorised officer* of a *criminal-law enforcement agency* (as defined in section 110A(1) of the TIA Act). This means only those agencies that are able to apply for a warrant to access stored communications are able to internally authorise the disclosure of prospective telecommunications data.

To reflect the increased privacy implications of access to prospective data, more restrictive conditions are attached to these authorisations, including:

- the authorised officer can only make an authorisation if they are satisfied the disclosure is reasonably necessary for the investigation of a *serious offence* (as defined in section 5D of the TIA Act) or an offence that is punishable by imprisonment for at least three years; and

[7] The new definition of *enforcement agency* introduced by the Data Retention Act implemented recommendation 5 in the 'Report of the Inquiry into Potential Reforms of Australia's National Security Legislation' and recommendation 21 in the 'Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014'
[8] **Attachment B** provides a list of *enforcement agencies*.
[9] Section 5 of the TIA Act defines an *authorised officer* as the head or deputy head of an enforcement agency, persons acting in those positions, and individuals holding positions within that agency who are authorised under subsection 5AB(1) and (1A).
[10] Subsection 178A(2) limits the ability to authorise the disclosure of telecommunications data for the purposes of locating persons who the Australian Federal Police or the Police Force of a State or the Northern Territory has been notified is missing.

[redacted]

- limiting the timeframe for which an authorisation may be in force to 45 days.

Access to telecommunications data by ASIO

In the case of ASIO, an *eligible person*[11] may authorise the disclosure of historical data (under section 175 of the TIA Act) or prospective data (under section 176 of the TIA Act) if satisfied that the disclosure would be in connection with the performance of ASIO's functions.

Journalist information warrants

The Data Retention Act introduced a journalist information warrant regime under Division 4C of Chapter 4 of the TIA Act. The regime requires ASIO and *enforcement agencies* to obtain a warrant when they are seeking the disclosure of telecommunications data to identify a journalist's source.[12]

The journalist information warrant regime requires that the *issuing authority*[13] or the Attorney-General (in the case of ASIO) must be satisfied that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source, having regard to a number of specified factors.

A Public Interest Advocate (who must be a retired senior judge or a security cleared Queen's Counsel or Senior Counsel) is required to consider and evaluate journalist information warrant applications made by ASIO and *enforcement agencies* pursuant to sections 180L and 180T, respectively, of the TIA Act. The Public Interest Advocate can make independent submissions to the Attorney-General or the issuing authority on the proposed undertaking in relation to each application. The role of the Public Interest Advocate is to provide an independent and impartial public interest assessment on the application of a journalist information warrant before it can be issued.

The Committee is also considering the journalist information warrant regime as part of the 'Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press'.

Privacy considerations

Section 180F[14] of the TIA Act requires *authorised officers* (to be distinguished from *eligible persons* in relation to ASIO) to consider privacy before issuing an authorisation for access to telecommunications data. Accordingly, an *authorised officer* must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use of telecommunications data is justifiable and proportionate, having regard to a range of matters including:

- the gravity of the conduct in relation to which the authorisation is sought (for example the seriousness of any relevant criminal offence)
- the likely relevance and usefulness of the information or documents, and
- the reason why the disclosure or use concerned is proposed to be authorised.

Oversight by the Commonwealth Ombudsman[15]

The Data Retention Act strengthened the oversight arrangements in the TIA Act to enable the Commonwealth Ombudsman to comprehensively assess compliance by *enforcement agencies* with the provisions governing the use and access to telecommunications data. Prior to the commencement of the Data Retention Act, there were no

[11] An *eligible person* is the Director-General of Security or the Deputy-General of Security. For historical telecommunications data, an *eligible person* includes an employee or an affiliate of ASIO who has been approved by the Director-General of Security to authorise disclosures of telecommunications data. For prospective telecommunications data, an *eligible person* includes a senior employee or affiliate of ASIO.
[12] *Eligible persons* of ASIO (section 180G) and *authorised officers* of enforcement agencies (section 180H) must not make an authorisation for the disclosure of telecommunications data, if they know or reasonably believe that the telecommunications data relates to a journalist or their employer, and a purpose of making the authorisation would be to identify a journalist's source, unless a Journalist Information Warrant is in force.
[13] Under section 6DC of the TIA Act, an issuing authority for the purposes of a journalist information warrant may be a Judge, magistrate or an Administrative Appeals Tribunal member who has been enrolled as an Australian legal practitioner for at least 5 years.
[14] The privacy protections provided for in section 180F were strengthened by the Data Retention Act in accordance with recommendation 25 in the 'Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014'
[15] The oversight regime introduced by the Data Retention Act implements relevant parts of recommendation 42 in the 'Report of the Inquiry into Potential Reforms of Australia's National Security Legislation'

[redacted]

independent oversight arrangements over the use of and access to telecommunications data under the TIA Act by *enforcement agencies*.

Schedule 3 of the Data Retention Act introduced a variety of measures into the TIA Act to facilitate the Ombudsman's oversight function, including:

- Record-keeping requirements to ensure agencies have relevant records to demonstrate the extent to which their use of powers was appropriate and complied with the requirements set out in Chapter 4 of the TIA Act (section 186A).
- Empowering the Ombudsman to enter an agency's premises at a reasonable time to inspect records and obtain any relevant documentation and information to carry out its oversight functions (subsection 186B(2)).
- Authorising the Ombudsman to require an officer of an *enforcement agency* to provide information in writing, and makes it an offence for a person to refuse to attend, give information or answer questions when required to do so (section 186C).
- Clarifying that agency officers are not prevented by other laws from providing necessary information or assistance to the Ombudsman (paragraph 186D(1)(a)).

Offences for unauthorised disclosures

Section 182 of the TIA Act creates an offence attracting a penalty of two years imprisonment where a person discloses or uses telecommunications data lawfully obtained under Chapter 4 of the TIA Act unless the use or disclosure is reasonably necessary for specified purposes. This includes (amongst others) specified purposes in connection with reporting and oversight functions, for the performance by ASIO of its functions, or for the enforcement of a criminal law (refer to section 182(2) and (3)). Similarly, section 182A of the TIA Act creates an offence for the disclosure or use of information about a journalist information warrant except for the purposes outlined in section 182B.

Access to telecommunications data under the *Telecommunications Act 1997*

Section 280 of the Telecommunications Act provides an exemption to the general prohibition on the disclosure of telecommunications data provided for in sections 276, 277 and 278 of that Act. Section 280 allows carriers and carriage service providers to disclose telecommunications data if the disclosure is required or authorised under law.[16]

Agencies that are defined as *enforcement agencies* under the TIA Act, and many other Commonwealth, State and Territory bodies that are not *enforcement agencies*, may have lawful authority to access telecommunications data under Commonwealth, State or Territory laws. Section 280 enables these laws to function as intended by providing an exemption from the prohibition against disclosing telecommunications data if it is in response to a lawful request from an agency under law.

However subsection 280(1B) clarifies that telecommunications data that is kept by a service provider solely for the purposes of complying with their data retention obligations under Part 5-1A of the TIA Act, cannot be disclosed under any circumstances to those bodies that are not *enforcement agencies.* Accordingly, section 280 does not expand the range of agencies with access to mandatorily retained data under the TIA Act.

[16] Home Affairs portfolio submission (Submission 21) to the PJCIS 'review of the mandatory data retention regime' provides further information in relation to access to telecommunications data under section 280 of the Telecommunications Act. pg. 34-35

Attachment A

Domestic access to Telecommunications Data in the TIA Act

The Telecommunications Act 1997 protects the privacy of Australians by, amongst other things, prohibiting service providers from using and disclosing information about customer's use of telecommunications services (s.276-278). Unauthorised disclosure of telecommunications data carries an imprisonment term of up to 2 years on conviction.

Chapter 4 of the Telecommunications (Interception and Access) Act 1979 sets out certain exceptions to the prohibitions in the Telecommunications Act to permit eligible Australian law enforcement and security agencies to authorise the disclosure of telecommunications data in specified circumstances.

Access by ASIO
Chapter 4, Division 3

Section 175: ASIO may authorise the disclosure of historical telecommunications data if they are satisfied that the disclosure would be in connection with the performance by ASIO of the functions.

Section 176: ASIO may authorise the disclosure of prospective telecommunications data if they are satisfied that the disclosure would be in connection with the performance by ASIO of the functions.

ASIO's compliance with the telecommunications data regime is independently overseen by the Inspector-General of Intelligence and Security.

Any authorisation made by an agency must be made by someone with the appropriate authority. In the case of ASIO this is an 'eligible person' **(subsections 175(2) and 176(2))**. In the case of an enforcement agency or criminal law-enforcement agency this is an 'authorised officer' **(section 5 and section 5AB)**

Access by enforcement agencies
Chapter 4, Division 4

Section 180F explicitly provides that officers must consider privacy when considering authorising the disclosure of telecommunications data.

Section 178: Enforcement agencies may authorise the disclosure of historical telecommunications data for the enforcement of the criminal law.

Section 178A: Police Forces may authorise the disclosure of historical telecommunications data for the purpose of finding a missing person.

Section 179: Enforcement agencies may authorise the disclosure of historical telecommunications data for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue.

Section 180: Criminal law-enforcement agencies may authorise the disclosure of prospective telecommunications data for the investigation of a serious offence (see: s 5D of the TIA Act) or an offence punishable by imprisonment for at least 3 years.

Journalist information warrants
Chapter 4, Division 4C

ASIO (**section 180G**) and enforcement agencies (**section 180H**) are required to obtain a journalist information warrant prior to authorising the disclosure of telecommunications data to identify a journalist's source.

The issuing authority must be satisfied that the public interest in issuing the journalist information warrant outweighs the public interest in protecting the confidentiality of the identity of the source.

Pubic Interest Advocates: The Prime Minister is able to declare persons to be Public Interest Advocates (PIA). PIAs are able to make submissions to the issuing authority about matters relevant to their decision to issue or refuse to issue a journalist information warrant.

The number of authorisations made by, and Journalist information warrants issued to, enforcement agencies in a particular year are reported in the TIA Act Annual Report.

Oversight by the Commonwealth Ombudsman
Chapter 4A

Section 186A requires enforcement agencies to keep specified information relating to authorisations and use and disclosure of telecommunications data for 3 years.

Section 186B: The Ombudsman is required to inspect the records of enforcement agencies to determine their compliance with the telecommunications data regime in Chapter 4 of the TIA Act.

Section 186C: The Ombudsman is able to obtain any relevant documentation and information to carry out its oversight function.

Section 186J: The Ombudsman must produce an annual report for the Minister detailing the results of their inspections of enforcement agencies. This report must be tabled in both Houses of Parliament within 15 sitting days of the Minister receiving it.

Data Retention Obligations
Part 5-1A

Section 187A and section 187C: Subject to certain exceptions, carriers, carriage service providers and internet service providers must retain specified telecommunications data for 2 years.

Section 187AA: Telecommunications data to be retained is split between 6 categories:
1) Subscriber Details
2) Source of a communication
3) Destination of a communication
4) Date, time duration of a communication
5) Type of communication or the service used in connection with a communication.
6) Location of equipment or a line used in connection with a communication.

Section 187BA requires service providers to ensure the confidentiality of retained telecommunications data by encrypting the information and protecting it from unauthorised interference or access.

Section 187LA provides that the Privacy Act 1988 applies to service providers (as if they were an organisation within the meaning of that Act) to the extent their activities relate to retained telecommunications data. For the purposes of the Privacy Act 1988, retained telecommunications data is taken to be personal information to the extent it relates to an individual or a communication to which the individual is a party.

Attachment B

Enforcement agencies – defined at subsection 176A(1) of the TIA Act	
Australian Criminal Intelligence Commission	Law Enforcement Conduct Commission
Australian Competition and Consumer Commission	Northern Territory Police
Australian Commission for Law Enforcement Integrity	New South Wales Crime Commission
Australian Federal Police	New South Wales Police Force
Australian Securities and Investments Commission	Queensland Corruption and Crime Commission
Corruption and Crime Commission (Western Australia)	Queensland Police Service
Department of Home Affairs[17]	South Australia Police
Independent Broad-based Anti-corruption Commission (Victoria)	Tasmania Police
Independent Commission Against Corruption (New South Wales)	Victoria Police
Independent Commissioner Against Corruption (South Australia)	Western Australia Police

[17] Paragraph 110A(1)(e) in conjunction with paragraph 176A(1)(a) means that the Department of Home Affairs (the Department) is an *enforcement agency* only in connection with the investigation by the Department of a contravention of certain legislation listed at subsection 110(1A).