

# Metadata and the Rule of Law

*This resource presents information about law reform to access telecommunications data (known as metadata) under the **Telecommunications (Interception and Access) Act 1979 (Cth)** - what it is, how it is used and who is authorised to use it.*

*The rapid development of telecommunications technology is a law reform issue because there is a need to ensure that law enforcement and intelligence agencies have sufficient powers to investigate and prevent crime.*




*The **rule of law** requires that agencies have powers to enforce the law. These powers need to be controlled, monitored and transparent in their use. This is to make sure that the power to access telecommunications is not abused by government agencies, and that a balance is maintained between having appropriate investigative powers, and the rights of the individual.*

## What is Metadata?

Metadata is part of a communication that describes the **who, what, when, where** and **how** of a communication. It does not include the content of a the communication itself.

To investigate crime and protect national security, government agencies have powers to access **telecommunications data** (the legal term in the TIA Act), known as **metadata** (the term everyone uses).

Metadata is usually created whenever a person sends or receives a communication over a phone or internet service. Consider the difference between content and metadata for these communications:

Communication	Content	Metadata
Phone call 	What is being said	<ul style="list-style-type: none"><li>* The name and phone number of the person who made/sent the call/ message and received the call/message</li><li>* The duration of the call</li><li>* Time the call was started and finished</li></ul>
SMS Message 	The text of the message	<ul style="list-style-type: none"><li>* Time the message was sent.</li><li>* The location of the device making the call.</li></ul>
Email 	The text of the email and the document attached to it.	<ul style="list-style-type: none"><li>* The email address the device is sent from and to</li><li>* The data volume used for the email</li><li>* The time the message was sent.</li></ul>

## Did you know?

As early as 1857, there was a law in NSW to protect the privacy of communications over the telegraph system, and an international agreement signed in 1865 called the **International Telegraph Convention**. Australia ratified this agreement in 1878. The International Telecommunication Union which is part of the United Nations, is the oldest intergovernmental organisation in the world.

## Important Terminology:

**The TIA Act** — Telecommunications (Interception and Access) Act 1979 (Cth) is the Australian law which controls access to telecommunications, and makes it an offence to access them unlawfully.

**Telecommunications data** — metadata.

**Telco** — a company offering telecommunications services.

**Law enforcement agency** — a government body which exists to investigate/prevent criminal activity.

**Intelligence agency** — a government body which exists to protect national security and collect intelligence.

**Interception warrants** — a court order from a Judge or AAT member that allows law enforcement agencies to access live communications.

**Stored communications warrants** — allows law enforcement to access stored communications.



## Why is Metadata Important?

Telecommunications data is often the first source of information for investigators. It is useful in helping to rule out potential suspects and prevent the need for more privacy intrusive investigative tools such as search warrants and interception warrants.

*"Telecommunications data becomes of significant value to assist in corroboration of the evidence on hand. That is, the movement of the offender before, during, after the offence, and their network etc" - the NSW Police submission to the Parliamentary review of data retention laws.*

The Murder of Jill Meagher—Metadata from Meagher's mobile phone was used to identify her killer. In the sentencing judgement Justice Nettle stated *'Fortunately, your effort to evade detection provide inadequate. Using CCTV and virtual telephone data obtained from, a number of sources, plus a host of witness statements, police were ultimately able to determine that you were the killer.'* - *Queen v Bayley (2013) VSC 313 (19 June 2013)*

## Telecommunications Companies ('telcos')

A telco is a company which offers telecommunications services such as mobile and fixed line phones, wired and wireless internet, or many other service that uses the telephone or internet networks to send messages. They are regulated by the **Telecommunications Act 1997** (Cth) .

### Telcos and Metadata

The rapid development of smart phone technology, and small handheld devices that can access the internet has changed the way telcos charge customers for services.

In the past telcos primarily charged users for calls and SMS messages based on the length of the call, and how many messages were sent. Metadata was recorded about all calls and messages and presented to the customer as a bill for service.

Since 2013 many telcos have started to offer services with unlimited calls, SMS messages or data which means keeping metadata is not as important for telcos.

Intelligence and law enforcement agencies like the Australian Crime Commission and ASIO found accessing metadata was problematic because the data kept by each telco was different, as well as the different lengths of time that data was kept by each company.

### Government Agencies

Since 1979, the number of agencies that can access telecommunications has expanded. Interception and stored communications warrants to access the **content** of communications can be applied for in the investigation of serious offences (see s5D TIA Act) - only law enforcement agencies have access to these warrants.

Access to **metadata**, however, has been much more widespread and can be used by many different government agencies in a broader range of investigations such as intelligence agencies, like ASIO, which collects intelligence in order to protect Australia's national security.

#### Delegated Legislation

The dataset refers to the information that a telco must keep for two years under the legislation.

When the Data Retention Bill was first presented to the Parliament in 2015, what data was required to be kept by telcos was to be determined through delegated legislation as a regulation to the TIA Act. This meant responsibility for creating and changing what would make up the dataset would be delegated to the Attorney General or the Minister responsible for the TIA Act. While there is oversight of the regulations that are made in Parliament—many felt that the dataset was too important to be delegated and that any changes to it should be brought before the Parliament to be debated. The Government agreed to this and the dataset (which is the information and documents telcos must keep) can be found in section 187AA of the TIA Act. Any future changes to the dataset would need to be presented as a Bill, and passed by the Parliament.

Delegated Legislation is a law made by the Executive. It can only be made when an Act authorises it.

## Legislative Reform: Mandatory Data Retention Regime

In 2015, in response to law enforcement and intelligence agencies, mandatory retention of metadata was introduced. Telcos are required under the legislation to keep **2 years worth of metadata** from all their services. The information must be stored securely and encrypted. The Act allows for approved law enforcement agencies to access metadata without a warrant, except for specific case of metadata relating to journalists.

The announcement of this legislation was met with significant criticism and concern regarding who would be able to access the metadata and the lack of protections for journalist and their sources. Many journalist and opponents of the Act argued that metadata can reveal just as much information about a person, the people they know and their habits as the content of the communication. The Attorney-General Department rejected this assessment as myth, however the ABC journalists, Will Ockendon interactive website of his metadata disputes the Attorney-generals position. Click [here](#) to explore.

### Review of the mandatory data regime

In 2019 the Parliamentary Joint Committee on Intelligence and Security (PJICIS) commenced a review of the mandatory data retention regime to assess its effectiveness. This review has been completed and the final report will be published by the end 2020.

1960

#### Telephonic Communications (Interception) Act 1960 (Cth)

The Attorney General authorised the Australian Security Intelligence Organisation (ASIO) to intercept telephone conversations in the interest of the security of the Commonwealth.

1979

#### The Telecommunications (Interception) Act 1979 (Cth)

This Act allowed interception of communications passing over all telecommunication. Interception were allowed at this point in narcotics investigations.

80s,90s & 00s

#### Amendments to the TIA Act

1987—State police forces and other 'eligible authorities' able to apply for interception warrants for investigating serious offences (S5D TIA Act)

2006—Stored Communications warrants introduced.  
2007—Agencies given powers to self-authorise access to telecommunications data.

2015

#### Telecommunications (Interception & Access) Amendment (Data Retention) Act 2015 (Cth)

Introduced of the "data retention bill".

2018

#### Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

## Who can Access Metadata?

Access to telecommunications data is regulated by Chapter 4 of the TIA Act, which permits 'enforcement agencies' to authorise telecommunications carriers to disclose telecommunications data where that information is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or the protection of the public revenue and to locate a missing person. Agencies approved to access metadata under the TIA Act **self-authorise access to data**. This involves a senior member of an agency giving permission to access metadata held by a telco. Some of the law enforcement agencies that can access data under section 110A of the TIA Act are:

Australian Federal Police	A police force of a state
Australian Criminal Intelligence Commission	Australian Commission for Law Enforcement Integrity
Australian Competition and Consumer Commission	Australian Securities and Investments Commission
Department of Home Affairs	Australia Commission Against Corruption

**The issues of Self Authorisation** It has been argued that there should be an independent person, separate from the law enforcement agency requesting the metadata, who approves access. It has been suggested judges could approve metadata request, or an independent body could be set up to make decisions about access to metadata. It has been argued that because of the sheer number of metadata requests made by law enforcement, that this however, would not be practical.

### How often is metadata accessed?

In the 2018-2019 Annual Report for the Telecommunications (Interception and Access) Act 1979, 20 enforcement agencies made 291,353 authorisations for disclosure of historical telecommunications data.

**Table 30: Number of authorisations made by an enforcement agency for access to existing information or documents in the enforcement of a criminal law – section 186(1)(a)**

Agency	Authorisations	
	17 / 18	18 / 19
ACCC	40	100
ACIC	7,498	6,536
ACLEI	413	393
AFP	19,432	16,818
ASIC	1,869	1,800
CCC (WA)	123	122
Home Affairs	3,598	3,283
IBAC	701	539
ICAC (NSW)	291	298
ICAC (SA)	288	220
LECC	376	459
NT Police	2,105	3,543
NSW CC	2,893	3,323
NSW Police	99,222	105,199
QLD CCC	1,271	1,009
QLD Police	25,014	23,693
SA Police	10,641	5,477
TAS Police	8,554	7,759
VIC Police	90,112	87,680
WA Police	21,338	23,102
<b>TOTAL</b>	<b>295,779</b>	<b>291,353</b>

### Non authorised agencies accessing Metadata

The Data Retention Bill 2015 removed access to metadata for all agencies except intelligence, law enforcement agencies, The Immigration and Broader Protection Department, the ACCC and ASIC.

However the Attorney General has discretion to grant access to agencies that are not considered approved agencies under the Act.

In making a decision about whether any agency should get access to metadata, the Attorney-General must consider:

- \* If access to metadata would be reasonably likely to assist in the investigation of serious contraventions of the law.
- \* If the agency complies with Australian Privacy Principles.
- \* Whether giving the agency the access to metadata is within the public interest

Agencies that have requested metadata include local councils (who request access to data to manage minor traffic offences, unlawful removal of trees, illegal rubbish dumping, and billposters), the RSPCA, the Environment Protection Authority, and state coroners.

\*The TIA Act Annual Report is released annually and contains details about law enforcement and other agencies' use of telecommunications warrants and metadata. It is available on the Attorney-General's Department website, the full report can be accessed here: <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance>

## Issues with Data Retention

Data retention creates tension with the concept of the **rule of law**. The rule of law requires that the law should be enforced. If the law enforcement do not have appropriate powers to investigate crime and enforce the law, can justice be done? On the other hand, the rule of law demands constant scrutiny of how government uses its power—to ensure it is fair, transparent and according to the law.

The fact that an enormous amount of data is kept for two years about any Australian who uses a telecommunications services, and access is self-authorised by government agencies, raises the concern that government might have **access to all people's data, not just those who are suspected of involvement in a crime**.

It also raises issues about an individual's right to privacy and civil liberties. The *International Covenant on Civil and Political Rights* (ICCPR) provides for the protection for individuals from arbitrary or unlawful interference with their privacy, family home or correspondence. Any assessment of the legitimacy of the mandatory data retention regime in relation to recognised international human rights, such as the right to privacy, must consider whether the laws are reasonably necessary and proportionate to achieving a legitimate purpose.

The TIA Act and the data retention regime have a legitimate purpose and contain many safeguards for people's privacy, and a degree of transparency through reporting requirements. However this does not mean that further changes or expansion of powers to access metadata should not be questioned and the current system should be reviewed to ensure that government agencies are not reaching beyond the powers they have in the legislation.

In public hearings in February 2020 at The Parliamentary Joint Committee on Intelligence and Security (PJCS) review of the metadata retention laws, the Commonwealth Ombudsman confirmed that law enforcement agencies are receiving URLs as part of the mandatory data retention regime, despite this practice being explicitly banned under the legislation. This example is of significant concern and was one of the major issues opponents of data retention had with the scheme.

## Journalist and Data Retention

Freedom of press is an essential aspect of a society which has the rule of law. Without independent journalists to investigate issues in the public interest, many important political, legal and social issues would not be known to the public. Having independent journalism is essential to the rule of law as it helps to hold government and other law enforcement agencies accountable.

### Key concern : Protection of Journalists sources

Many journalist have voiced concern that Australian metadata laws have a freezing effect on anyone who wish to give information to a journalist. The potential for enforcement agencies to discover journalist sources through metadata raises some controversial legal and ethical issues. Journalist adhere to a professional code of ethics that means they will not reveal their sources. Clause 3 of MEAA's *Journalist Code of Ethics* requires confidences to be respected in all circumstance. However if law enforcement can access anyone's metadata then they may be able to identify journalist sources. This is significant because some sources may be providing journalists with information about government behaviour and alleged corruption. The legal issue in this situation is that many such disclosures of government information is illegal, and law enforcement would have good reason to identify a leak.

*"Our major fear is that the new regime will crush investigative journalism in Australia and deal a serious blow to freedom of speech and press freedom. A healthy democratic society requires robust free speech and a free and vigour press to hold governments accountable. To fulfill this critical role, the press need to be able to engage with confidential sources".* Professor David Weisbord, Chair of the Australian Press Council, Media release, 11 March 2015.

## Safeguards for Journalists in the TIA Act

The Data Retention Act established the Journalist Information Warrant (JIW) scheme. This requires enforcement agencies to obtain a warrant prior to authorising the disclosure of telecommunications data to identify a journalists' source. A warrant will be granted where the Minister believes the interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the source. In 2017-19 TIA Act Annual Report two JIW were issued with 58 metadata request made.

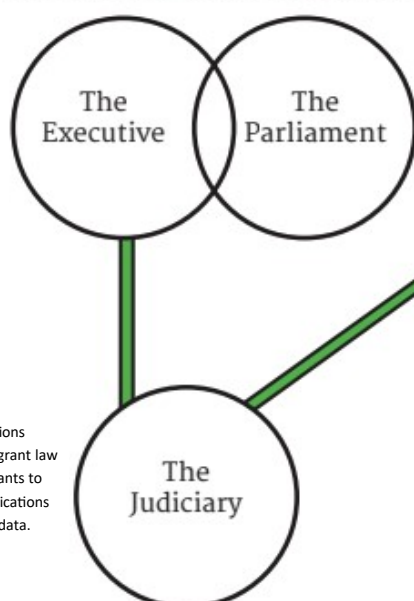
This scheme has been criticised especially in light of revelations in 2017 that the Australian Federal Police had accessed a journalist's metadata without a warrant. An audit by the Commonwealth Ombudsman found that Australian Federal Police did not destroy all copies of phone records it obtained unlawfully, without a warrant, for the purpose of identifying the journalist's source. The Commonwealth Ombudsman report can be found [here](https://www.ombudsman.gov.au/data/assets/pdf_file/0034/96748/A-report-on-the-Commonwealth-Ombudsmans-inspection-of-the-Australian-Fe....pdf).

## The Separation of Powers & Access to Telecommunications

Law enforcement and intelligence agencies perform functions and use powers defined by Acts of Parliament.

Government Ministers have power to make certain decisions eg the Attorney General authorises **interception warrants** for ASIO.

Judges make decisions about whether to grant law enforcement warrants to intercept communications and access stored data.



Parliament passes laws to ensure that law enforcement have the powers they need to investigate crime.

Laws include safeguards to ensure powers cannot be abused.

Debates in Parliament about these laws often see arguments about the right balance between granting powers and safeguards.

