Telecommunications Companies (telcos)

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

Until 1997, the majority of telecommunications services and infrastructure were owned by the Australian Government. Now there are many different companies offering these services such as Telstra, Optus, Vodaphone, iiNet, and TPG.

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 the service.

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

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

Government Agencies

Federal, State and Territory Police forces, are essential in ensuring crimes are investigated and those accused are placed before the courts. They also have the responsibility to prevent crime and to protect the community from harm.

Intelligence agencies, like ASIO, collect intelligence in order to protect Australia's national security.

The Parliament ultimately decides what powers to give these agencies and how the law will balance the need to equip agencies with appropriate powers to do their job, with the effect these power could have on individuals, and society.

The Importance of Metadata in Criminal Investigations

The Murder of Jill Meagher – metadata from Meagher's mobile phone was used to identify her killer, read Nettle J at paragraph 12 of the sentencing judgment in **Queen v Bayley [2013] VSC 313 (19 June 2013)**:

> *"Fortunately, your efforts to evade detection proved inadequate. Using CCTV footage collected from cameras at various points along Sydney Road, Brunswick, City Link records of vehicles passing under the Moreland Road gantry 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."*

The Commissioner of the **Australian Federal Police** (AFP), Andrew Colvin giving evidence to the **Parliamentary Joint Committee on Intelligence and Security** on 17/12/2014:

> *"Looking at AFP investigations commenced between July and September of this year, 2014, I can advise that telecommunications data has been used in 92 per cent of counterterrorism investigations, 100 per cent of cybercrime investigations, 87 per cent of child protection investigations and 79 per cent of serious organised crime investigations."*

Law Reform: Accessing Telecommunications

Key Issue: Mandatory Retention of Metadata

The Federal Attorney-General's Department had been looking at introducing data retention since before 2012, and the same year the Parliamentary Joint Committee for Intelligence and Security recommended data retention of metadata be introduced.

In 2015, in response to calls from intelligence and law enforcement agencies, mandatory retention of metadata was introduced. This means that telcos are required to keep 2 years worth of metadata from all their services. Telcos have been given until the end of 2016 to design systems to protect, store and allow access to this data.

The original Bill presented to Parliament to introduce data retention posed some concerns:

- **how would metadata be defined in law**?
- **who would be able to access metadata**?
- and the **absence of protections for journalists and their sources.**

The Parliamentary Joint Committee on Intelligence and Security reviewed the Data Retention Bill and made 39 recommendations, all of which were accepted by the Government.

It is important to note that while there was debate over particular matters in the Bill there was bi-partisan support for data retention.

The TIA Act requires that a report is released to the public each year and provides statistics on the use of powers in the TIA Act such as:

interception warrants (content of communications)

stored communications warrants (content of communications) granted to agencies by judges.

The number of self-authorisations to access **telecommunications data** (metadata)

1960

Telephonic Communications (Interception) Act 1960 (Cth)

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

In 1960, telecommunications could only be accessed by intelligence agencies!

Access has been granted to law enforcement over the years to allow them to keep up with the development of technology and remain effective in investigating crime.

' "**the security of the Commonwealth**" means the protection of the Commonwealth and the Territories from acts of espionage, sabotage or subversion, whether directed from, or intended to be committed, within the Commonwealth or not;'

– Section 3, *Telephonic Communications (Interception) Act* 1960 (Cth)

1979

The Telecommunications (Interception) Act 1979 (Cth)

In 1979 the Telecommunications (Interception) Act was passed and allowed interception of communications passing over all telecommunications systems. 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 (see s5D TIA Act)

2006 - Stored Communications Warrants introduced

2007 - Agencies given power to self-authorise access to telecommunications data (metadata)

2015

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

Referred to above as 'the Data Retention Bill'.

In March 2015, the TIA Act was amended to require telecommunications companies to retain two years worth of telecommunications metadata. Law enforcement agencies self-authorise access to metadata.

How is metadata accessed by law enforcement in 2016?

Law enforcement agencies permitted by the TIA Act may **self authorise** access to metadata.

This involves the investigating officer filling out a form, and a high-ranking member of their agency approving access to the metadata. A request is then made to the telco for the metadata, and the agency pays for the cost of accessing the data.

Rule of Law Institute of Australia © 2016

Who Can Access Metadata?

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:

- the enforcement of a criminal law
- the enforcement of a law to impose a pecuniary($) penalty
- for protecting public revenue

Organisations such as the RSPCA and local councils have been granted the power to self-authorise access to metadata. The cost of accessing the data prohibits wide-spread surveillance – many opponents of mandatory retention of metadata argue that access to metadata should be limited only to law enforcement agencies.

How often is metadata accessed and by who?

The following data is from the TIA Act Annual Report for 2014/15*

	13/14	14/15
Pecuniary Penalties or Protecting Public Revenue		
No. of authorisations made by a Law Enforcement Agency	6,380	4,554
No. of authorisations made by a Commonwealth Agency	1,866	1,744
No. of authorisations made by a State or Territory Agency	2,152	2,197
Total	**10,398**	**8,495**

	13/14	14/15
Enforcing Criminal Law		
No. of authorisations made by a Law Enforcement Agency	314,587	341,597
No. of authorisations made by a Commonwealth Agency	8,653	12,128
No. of authorisations made by a State or Territory Agency	1,020	1,116
Total	**324,260**	**354,841**

***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 shows data on the number of authorisations made by each agency, see:**
https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/AnnualReports.aspx

Intelligence and law enforcement agencies have described the loss of access to metadata as 'going dark' meaning that they would be unable to track current and developing threats to national security, as well as criminal activities.

State or Territory Agencies

Consumer and Business Services (SA), Corrective Services NSW, Dept. of Commerce (WA), Dept. Economic Development, Jobs, Transport & Resources (Vic), Dept. Environment Regulation (WA), Dept. Environment, Land, Water & Planning (Vic), Dept. Justice (Corrections Victoria), Environment Protection Authority (NSW), Legal Services Board (Vic), Office of Environment and Heritage (NSW), Roads and Maritime Services NSW, RSPCA QLD, RSPCA Tas., RSPCA Vic., The Hills Shire Council, Transport Accident Commission (Vic.), Workcover NSW, Worksafe Victoria, ACT Revenue Office, Bankstown City Council, City of Darebin, Consumer Affairs Vic., Dept. Environment & Heritage Protection (QLD), Dept. Agriculture and Fisheries (QLD), Dept. Fisheries (WA), Dept of Justice (Sheriffs Office Victoria), Dept. Mines and Petroleum, Dept. Parks & Wildlife (WA), Dept. Primary Industries (NSW), Harness Racing NSW, Harness Racing Vic., Health Care Complaints Commission (NSW), Ipswich City Council, Juvenile Justice NSW, Knox City Council, Offices of Fair Trading in NSW & QLD, Offices of State Revenue in NSW and QLD, Office of Liquor & Gaming Regulation (QLD), Primary Industries & Regions (SA), Racing and Wagering WA, Racing NSW, Racing QLD, State Revenue Office Vic., Taxi Services Commission (Vic.), Wyndham City Council.

Law Enforcement Agencies

The following is a complete list of agencies who self-authorised access to metadata in 2014/15:

Australian Crime Commission, Australian Commission for Law Enforcement Integrity, Australian Federal Police, Crime and Corruption Commission (QLD), Crime and Corruption Commission (WA), Independent Commission Against Corruption (NSW), Independent Commission Against Corruption (SA), Broad-based Anti-corruption Commission, NSW Crime Commission, Police Integrity Commission NSW, all state and territory police forces.

Metadata and the Rule of Law

This resource presents information about law reform to access to 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 content and metadata for some common types of telecommunications:

Communication	Content	Metadata
Phone call	What is being said	• The name and phone number of the person who made/sent the call/ message and received the call/message • the duration of the call
SMS Message	The text of the message	• time the call was started and finished • time the message was sent • the location of the device making the call
Email	The text of the email and documents attached to it	• The email address the device is sent from and to • time the message was sent • the data volume used for the email (did they send a large file?)

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.

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 now, is the oldest intergovernmental organisation in the world.

Further reading and resources on this topic and other rule of law issues are available at:

www.ruleoflaw.org.au/education/metadata/

RULE OF LAW INSTITUTE OF AUSTRALIA

Issues with Data Retention

Data retention creates tension within the concept of the rule of law. The rule of law requires that the law should be enforced – if law enforcement do not have appropriate powers to investigate crime, can justice be done?

However, the fact that an enormous amount of data is kept for two years about any Australian who uses a telecommunications service, and that access to that power 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.

Currently, it is not possible for law enforcement to monitor all people at all times – **this would be very expensive, and is not permitted under the current legislation**.

Although the TIA Act contains many safeguards for people's privacy, and has a degree of transparency through reporting requirements – this does not mean that further changes or expansion of powers to access metadata should not be questioned.

The rule of law demands constant scrutiny of how government uses its power – this is how we can live in a free society, while having government agencies that use powers appropriately, according to the law.

A few years after the first personal computer (PC) in 1976, the Apple I, Sony released the first low cost portable "stereo walkman" – it played cassette tapes, had a built in microphone, and the tapes themselves only had 30 to 45 minutes of audio per side. The walkman hit shelves the same year the TIA Act was passed.

The first mobile phone network in Australia commenced operation in Melbourne in 1981 – a mobile phone handset cost approx. $5000, weighed 12kg, and used the car's horn and headlights to notify the owner when they were receiving a call. The first handheld mobile phone did not arrive in Australia until 1987, and were so large they are now affectionately referred to as 'bricks'. **Read:** http://www.smh.com.au/digital-life/mobiles/40-years-on-mobile-phones-still-pushing-consumers-buttons-20130404-2h9ua.html

Who gets Access to Metadata?

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.

In March 2015, the introduction of data retention removed access to metadata for all agencies except intelligence and law enforcement agencies, the Immigration and Border Protection Department, the ACCC and ASIC.

As of January 2016, a freedom of information request made by ZDNet, a technology news website, to the Attorney-General's Department revealed that 61 local, state and federal agencies have applied to the Attorney-General for access to metadata. (http://www.zdnet.com/article/61-agencies-after-warrantless-access-to-australian-telecommunications-metadata/)

In making a decision about whether an 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 the Australian Privacy Principles, and other privacy legislation
- if the agency can satisfy the same obligations as a law enforcement agency in accessing and storing accessed data, and
- whether giving the agency access to metadata is in the public interest.

At March 2016, there is no information on whether the 61 agencies have been granted access by the Attorney-General. Such declarations would be available on ComLaw when and if they are made.

Criticisms Length of Time

Many of the critics of data retention say that 2 years is too long to keep metadata.

In 2014, the European Court of Justice struck down the European Union's data retention scheme, which held data from six months to two years, because it interfered with the right to privacy under EU Law, did not contain sufficient safeguards and was disproportionate to its stated objectives.

Criticisms about Self-Authorisation

Some people argue that there should be an independent person, separate from the law enforcement agency requesting the metadata, who approves access.

It has been suggested that judges could approve metadata requests, 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 would not be practical.

In the case of using judges to decide on access, law enforcement have argued that the sheer number of requests they make for metadata may make it impossible for judges to perform this function.

The Dataset and Delegated Legislation

The dataset is the list of metadata that must be kept by a telco. In the original Data Retention Bill presented to the Parliament in 2015, the dataset was to be made through delegated legislation as a **regulation** to the TIA Act.

This meant responsibility for creating and changing the dataset would be delegated to the Attorney-General or the Minister responsible for the TIA Act.

While there is oversight of 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 change and the data set can be found in Section 187AA of the TIA Act. Any future changes to the data set would need to be presented as a Bill, and passed by the Parliament.

One of the key concerns raised in the debate about data retention was whether the dataset would include information that showed people's internet browsing history. The Government has stated that the current dataset does not include websites visited.

What is delegated legislation?

Delegated legislation is a law made by the Executive.

Delegated legislation can only be made when an Act authorises it.

A regulation is a common form of delegated legislation.

Journalists and Data Retention

Freedom of the 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.

Key Issue: Protection of Journalists' Sources

Professional journalists who work for newspapers, online news services or any other publication tend to adhere to a professional code of ethics that means they will not reveal the identity of their sources.

Many journalists have argued that retention of metadata will have a 'freezing effect' on anyone who wishes to give information to a journalist.

Journalists have also argued that metadata can reveal just as much information about a person, the people they know, and their habits as the content of a communication – the Attorney-General's Department has argued that this is a myth, however, ABC Journalist, Will Ockenden's interactive website with his own metadata convincingly disputes this. See: http://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152

Why is this a problem?

This can become a controversial legal and ethical issue when journalists investigate the actions of government – for example, if a journalist is receiving and publishing information from a government employee about alleged corruption in government.

While there are some protections in the Public Interest Disclosure Act 2013 (Cth) for whistleblowers who disclose information – journalists have argued that data retention will mean that law enforcement can request the metadata of anyone who might have leaked information without accessing the journalist's metadata.

The legal issue here is that many disclosures of government information can be illegal, and law enforcement will have good reason to identify a leak. It is appropriate that law enforcement should investigate leaks of secret or confidential information. Whether or not a leak to a journalist is in the public interest is a hotly debated topic.

Safeguards for Journalists in the TIA Act

In response to criticism by journalists regarding the effect data retention could have on them, the data retention Bill was amended to require law enforcement to apply to the Federal Attorney-General for a warrant before they can access a journalist's metadata.

Journalists argue this protection is not sufficient and that law enforcement could request a wide range of metadata that could identify their sources without having to access the journalists' metadata.

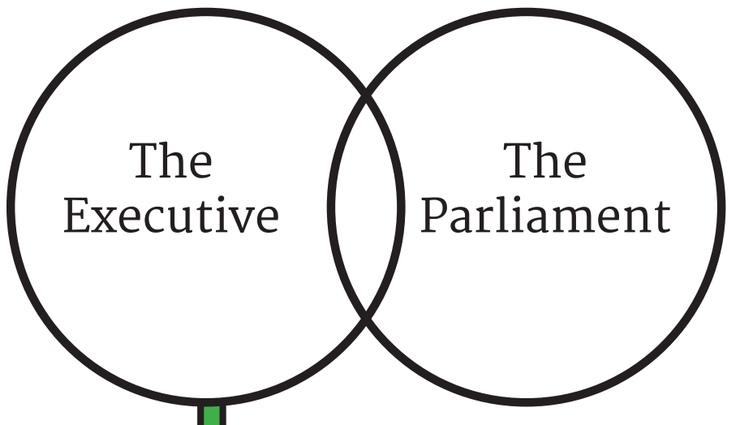
> "Respect for truth and the public's right to information are fundamental principles of journalism. Journalists describe society to itself. They convey information, ideas and opinions, a privileged role. They search, disclose, record, question, entertain, suggest and remember. They inform citizens and animate democracy. They give a practical form to freedom of expression. Many journalists work in private enterprise, but all have these public responsibilities. They scrutinise power, but also exercise it, and should be accountable. Accountability engenders trust. Without trust, journalists do not fulfil their public responsibilities.
>
> …
>
> 3. Aim to attribute information to its source. Where a source seeks anonymity, do not agree without first considering the source's motives and any alternative attributable source. Where confidences are accepted, **respect them in all circumstances**."
>
> The MEAA Journalist Code of Ethics

> "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. It will dissuade whistleblowers and confidential sources from engaging with the media, and similarly it will discourage what once were 'anonymous tips' – despite the fact that many such revelations have proved over the years to contain critical material that is wholly in the public interest to ventilate since it may expose corruption or misconduct.
>
> A healthy democratic society requires robust free speech and a free and vigorous press to hold governments and other powerful interests to account. In order to fulfil that critical role, the press needs to be able to engage with confidential sources"
>
> – Professor David Weisbrot, Chair of the Australian Press Council, Media Release, 11 March 2015.

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 powers to make certain decisions. For example, the Attorney-General authorises **interception warrants** for ASIO.

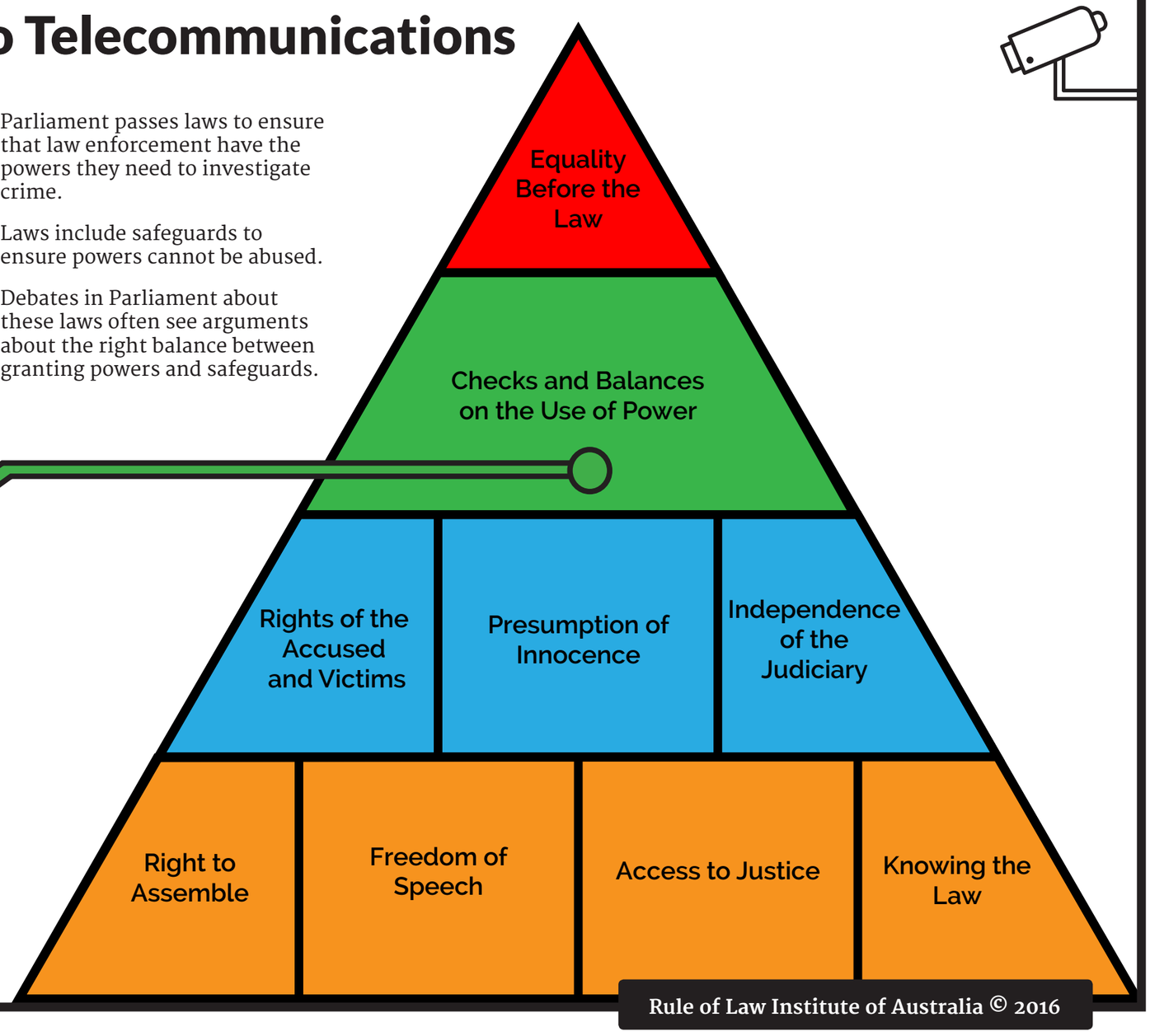


Parliament passes laws to ensure that law enforcement have the powers they need to investigate crime.

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.

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



Rule of Law Institute of Australia © 2016