Notes:

The Rule of Law Institute of Australia is an independent, not for profit, non-partisan organisation which promotes discussion about rule of law issues in Australia.

ACCESS GRANTED

TELECOMMUNICATIONS DATA AND THE RULE OF LAW

1

Rule of Law Issues

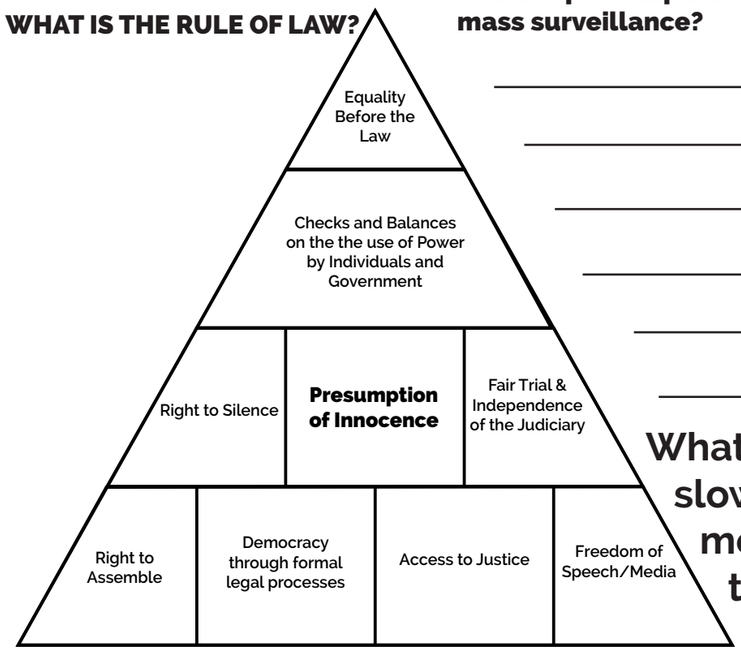
- The Presumption of Innocence

- Checks and Balances on the use of Power by Individuals and Government

2 **Possible Effects of Surveillance:**

1. Diminishes the presumption of innocence
2. _____
3. _____
4. _____

WHAT IS THE RULE OF LAW?



Can the presumption of innocence survive the era of mass surveillance?

_____

_____

_____

_____

_____

_____

_____

What does a backpack, a slow cooker, quinoa, and metadata have to do with terrorism?[1] (See references)

3

Conflict between:

Rights of the individual:
Privacy and Civil Liberties

AND

The needs of the state:
Safety and Security

4

"We were able to track Jill Meagher's phone through this data to where her location was, to where she was buried, and show that only one phone came back."[2]

LAW REFORM ISSUE - MANDATORY RETENTION OF METADATA

WHAT ARE TELECOMMUNICATIONS?

Telecommunications are the use of electronic equipment such as:

- mobile phones,
- computers,
- pagers,
- fax machines

to transmit and receive data such as: sound, images, text, and computer code.

WHY ACCESS TELECOMMUNICATIONS?

Having these communications allows law enforcement to:

1. Monitor communications between people suspected of crime.
2. Establish a person's whereabouts and associates.
3. Predict or prevent criminal activity.
4. Identify members of criminal organisations.

The **TIA Act**, **T**elecommunications (**I**nterception and **A**ccess) **Act** 1979 (Cth) gives government agencies powers to access telecommunications.

POWER TO ACCESS CONTENT

Interception Warrants and **Stored communications warrants** allow law enforcement agencies to access the **content** of communications

Examples of the content of communications are listening to a phone call as it happens or obtaining the text of an email or SMS message.

POWER TO ACCESS METADATA

Metadata - the when, where and who a communication is sent by and to, which does not include the content of a communication.

It can be difficult to tell the difference between the **content of a communication** and its **metadata**. Metadata can reveal information about the content and can be as informative as the content itself.

The legal term in the TIA Act for metadata is **telecommunications data**.

CHANGES TO THE TIA ACT IN 2015

The Commonwealth Government amended the TIA Act to require:

MANDATORY RETENTION OF METADATA FOR 2 YEARS

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

WHAT DOES THIS MEAN LEGALLY?

1. Telecommunications companies must **keep metadata for 2 years**
2. Criminal enforcement agencies can **self-authorise to access metadata**.

WHAT DATA MUST BE KEPT?

1. Details about the person who owns the service/account.
2. The device used (a phone, a computer, an IP address).
3. The destination and recipient of the communication .
4. Date, time, duration of the communication.
5. Type of communication (SMS or email or voice call).
6. Location of the device at the start and end of the communication.

PROCESS FOR ACCESSING METADATA

1. An investigator requests metadata.
2. A senior officer or official in the enforcement agency can authorise access to metadata.
3. A telecommunications company must then be approached for the data, and they charge a fee to retrieve it.
4. Requests for authorisations must be recorded and are reported by the Attorney-General's Department each year in the **TIA Act Annual Report**[3].

Is it too easy for law enforcement to access this data? Should access to metadata require a warrant from a court the same as for interception warrants for the content of communications?

324 260

The number of authorisations for access to metadata for criminal investigations in 2013/14.[3]

There is no data available on how many requests for metadata are refused.

THE CASE AGAINST DATA RETENTION

1. It is a disproportionate response with unproven benefits.
2. It is an unjustifiable invasion of privacy.
3. It leaves journalists sources vulnerable.
4. There is a risk of data breaches by hackers.
5. Telecommunications companies are concerned about the cost which is predicted by the Government to be around $400 million.

THE RULE OF LAW & DATA RETENTION

1. Access to metadata is an important tool for law enforcement in investigating crime.
2. Access to metadata should have greater oversight than self-authorisation.
3. There must be more detailed, rigorous and transparent reporting about the use and effectiveness of these powers.
4. Freedom of the press and the protection of journalists sources is an unresolved issue. A Federal Senate Committee is set to consider this in the second half of 2015.

CENTRAL QUESTION?

To what extent is the mandatory retention of data change our understanding of the presumption of innocence?

Does self authorisation to metadata give law enforcement too much unchecked power?

Notes:

"you have to watch every little thing you do because someone else is watching every little thing you do. ... I'm scared. And not of the right things."[1]

REFERENCES

1. Michele Catalano, '**My family's Google searching got us a visit from the counterterrorism police**', The Guardian, 02/08/2013. a

2. Ron Iddles, Secretary of the Victorian Police Association. ABC News, '**Data retention inquiry: Victorian police defend regular access to phone, internet records**', 14/01/2015

3. Attorney-Generals Department, TIA Act Annual Report 2013-14, https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/Telecommunications-Interception-and-Access-Act-1979-Annual-Report.pdf