Notes:

RULE OF LAW
INSTITUTE OF AUSTRALIA
RULEOFLAW.ORG.AU

ACCESS GRANTED

TELECOMMUNICATIONS DATA AND THE RULE OF LAW

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

2 **Rule of Law**
- The Presumption of Innocence
- Checks and Balances on the use of Power by Individuals and Government

3 **Conflict**
- Safety and Security (the needs of the state) against
- Privacy and Civil Liberties (rights of the individual)

4 "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]

What does a backpack, a slow cooker, quinoa, and metadata have to do with terrorists?

Possible Effects of Surveillance:

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

Definition of Metadata…

NOTES:

5 "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]

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

Legislation

THE TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979 (CTH)

FOR SHORT **THE TIA ACT**

What are telecommunications?

Telecommunications are the use of electronic equipment such as:

mobile phones, computers, pagers, fax machines, satellites

to transmit and receive data such as:

sound, images, text, computer code

Statistics on Use of Metadata

319874 authorisations for metadata in **criminal investigations** in 2012/13, very few refusals/withdrawals (close to zero)

including the following number from:

Federal Police - **25582**

NSW Police - **119705**

Bankstown City Council - **5**

RSPCA - **23**

TIA Act Annual Report 2013, pp.47-49:

http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Annualreports.aspx

Mandatory Data Retention of Metadata

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 will amend the **TIA Act**:

- Companies (Telcos like Telstra, Optus, iiNet) must retain metadata for a **minimum of 2 years**
- Initially limits access to **criminal enforcement agencies**, but more can be declared by the Attorney-General

Why access telecommunications?

Having these communications allows law enforcement to:

- monitor communications between people suspected of crime
- establish a person's whereabouts and associates
- predict or prevent criminal activity
- identify members of criminal organisations

Legal Options for Accessing Communications

1. Interception and Stored Communications Warrants

The **content** of communications.

Example: listening to a phone call as it happens or reading what a text message/email says

WARRANT ISSUED BY A COURT

2. Telecommunications Data Authorisations (Metadata)

Metadata is the when, where and who a communication is sent by and to

Example: the name of the sender and recipient of an SMS & location when sent

SELF-AUTHORISED BY THE AGENCY

The Case Against Data Retention

Who is against it?

- **Civil liberties organisations** - NSW Council for Civil Liberties
- **the Greens** - in particular Senator Scott Ludlum
- **Journalists** - Paul Farrell at the Guardian

Why?

- Disproportionate response and unproven benefits
- Unjustifiable invasion of privacy
- Journalists sources vulnerable
- Risk of data breaches by hackers

Telecommunications Companies are concerned because of effect on consumers and potential cost predicted by the Government to be around $400 million

The Rule of Law & Data Retention

- Access to metadata is an **important tool for law enforcement** in investigating crime
- access to metadata should require **more than a "rubber stamp"** self-authorisation
- There must be more **rigorous and transparent reporting** of the use of these powers. This is included in the new Bill, but we need to wait and see
- **freedom of the press** issue is unresolved, a Committee will examine this later in the year

What is the metadata dataset?

Data retained about communications includes:

- **details about the person** who owns the service/account
- the **device used** (a phone, a computer, an IP address)
- the **destination** and recipient of the communication
- date, time, duration of the communication
- **type** of communication (SMS or email or voice call)
- **location** of the device at the start and end of the communication

Process for Getting 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 the police a fee to retrieve it
4. Requests for authorisations must be recorded and are reported by the Attorney-General's Department each year

Is this process too "rubber stamp" like, should access to metadata require a warrant and therefore judicial oversight?

The unnerving feeling that our **presumption of innocence** is in some way diminished by **mandatory data retention** seems impossible to avoid.

There is no question it is a valuable tool.

But scrutiny of these laws and how they operate must continue after they are passed.

Further reading on Data Retention and changes to telecommunications interception

No warrants needed to access Opal Card records: http://www.smh.com.au/digital-life/consumer-security/no-warrants-needed-to-access-opal-card-records-20140714-zt02j.html

Why is data retention an option in Australia after Europe says no? http://www.smh.com.au/technology/technology-news/why-is-data-retention-an-option-in-australia-after-europe-says-no-20140414-zqup1.html

The Guardian Australia's submission to revision on the TIA Act Inquiry on the freedom of journalists: http://www.aph.gov.au/DocumentStore.ashx?id=c7f-7c00b-33f5-45d6-9d31-8de565c69c74&subId=251377

The NSW Council for Civil Liberties submission to the TIA Act Inquiry, see p.6 for info on data retention: http://www.aph.gov.au/DocumentStore.ashx?id=4a-7c3aee-1a1c-44e2-a806-28fb25a5be1d&subId=251942

Notes: