ACCESS GRANTED…

TELECOMMUNICATIONS DATA (METADATA)
AND THE RULE OF LAW

www.ruleoflaw.org.au
What is the Rule of Law?

- Limits on the use of power
- People can only be punished through the law

Diagram:

- Equality Before the Law
- Checks and Balances on the use of Power by Individuals and Government
- Presumption of Innocence
- Fair Trial & Independence of the Judiciary
- Access to Justice
- Freedom of Speech/Media
- Democracy through formal legal processes
- Right to Assemble
RULE OF LAW REQUIRES THAT LAWS PROVIDE LIMITS ON THE:

- POWER OF GOVERNMENT

- BEHAVIOUR OF THE INDIVIDUAL

TECHNOLOGY GIVES PEOPLE THE POWER TO COMMUNICATE IN WAYS IMPOSSIBLE 30 YEARS AGO
SYLLABUS LINKS

1. INTERCEPTION WARRANTS
2. TELECOMMUNICATIONS DATA (METADATA) & MANDATORY DATA RETENTION

YEAR 11 - INDIVIDUAL AND THE LAW
YEAR 12 - CRIME, POLICE INVESTIGATION POWERS
MASS SURVEILLANCE...

SAFETY AND SECURITY
Needs of the state

VS

PRIVACY AND CIVIL LIBERTIES
Rights of the Individual
TELECOMMUNICATIONS
SERVICE PROVIDERS
TELECOM, OPTUS

ACCESS POINTS
WIFI, HOTSPOTS, ADSL, NBN, 3G, 4G, LTE,
INTERNET CAFÉ, HOTEL, AIRPORT

DEVICES
HOME PHONE, BUSINESS PHONE, FAX,
SMART PHONE, DESKTOP COMPUTER, LAPTOP,
TABLET, GAMING CONSOLE

TELECOMMUNICATIONS
SERVICE PROVIDERS
TELSTRA, OPTUS, VODAFONE, iiNET, INTERNODE, ETC.

ANCILLARY PRODUCTS
SMART PHONE APPLICATIONS, VOIP (VIBER ETC.), IM, EMAIL

ANCILLARY PROVIDERS
APPLE, GOOGLE, MICROSOFT, BLACKBERRY,
INDEPENDENT DEVELOPERS

EXPANSION OF TECHNOLOGY
BIOMETRICS, SMART DEVICES (WATCHES & GLASSES),
CLOUD, UNKNOWN?

2010
ACCESS POINTS
WIFI, HOTSPOTS, ADSL, NBN, 3G, 4G, LTE,
INTERNET CAFÉ, HOTEL, AIRPORT

DEVICES
HOME PHONE, BUSINESS PHONE, FAX,
SMART PHONE, DESKTOP COMPUTER, LAPTOP,
TABLET, GAMING CONSOLE

TELECOMMUNICATIONS
SERVICE PROVIDERS
TELSTRA, OPTUS, VODAFONE, iiNET, INTERNODE, ETC.

ANCILLARY PRODUCTS
SMART PHONE APPLICATIONS, VOIP (VIBER ETC.), IM, EMAIL

ANCILLARY PROVIDERS
APPLE, GOOGLE, MICROSOFT, BLACKBERRY,
INDEPENDENT DEVELOPERS
TARGETED ADVERTISEMENTS BASED ON BROWSING HABITS
“What the hell is quinoa?”

New York woman visited by police after researching pressure cookers online

Long Island resident said her web search history and 'trying to learn how to cook lentils' prompted a visit from authorities but police say search was prompted by tipoff.

Adam Gabbatt in New York

@adamgabbatt

Friday 2 August 2013 06.59 AEST
QUERY STRING, IS IT CONTENT OR METADATA?
“I felt a sense of **creeping dread** take over. What else had I looked up?

What kind of searches did I do that alone seemed **innocent enough** but put together could make someone suspicious?

Were they judging me because my house was a mess (Oh my god, the joint terrorism task force was in my house and there were dirty dishes in my sink!).

**Mostly I felt a great sense of anxiety. This is where we are at. Where you have no expectation of privacy.** Where trying to learn how to cook some lentils could possibly land you on a watch list.

**Where 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.”**

Michele Catalano, ‘My family’s Google searching got us a visit from counterterrorism police’, The Guardian, 02/08/2013, [link](#)
POSSIBLE EFFECTS OF SURVEILLANCE ON THE INDIVIDUAL

- DIMINISHES THE PRESUMPTION OF INNOCENCE
- INVADES PRIVACY
- LAW ENFORCEMENT COULD USE DATA TO PROVE INNOCENCE OF AN ACCUSED?
- ADVERSE EFFECTS ON FREEDOM OF THE PRESS IF JOURNALISTS’ SOURCES ARE REVEALED
WHAT ORGANISATIONS?

LAW ENFORCEMENT

• NSW POLICE
• AUSTRALIAN FEDERAL POLICE (AFP)
• AUSTRALIAN CRIME COMMISSION (ACC)

INTELLIGENCE & SECURITY

• AUSTRALIAN SECURITY AND INTELLIGENCE ORGANISATION (ASIO)
• AUSTRALIAN SPECIAL INTELLIGENCE SERVICE (ASIS)
Legislation

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

FOR SHORT THE TIA ACT
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

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
Difficult to define metadata

- Some argue it is pointless to draw a distinction between the **content of a communication** and the **metadata** it creates.

- The Government has developed a dataset which defines what metadata is for the new **data retention Bill**.

- They have responded to criticism and the dataset will be in the **primary legislation** (The TIA Act), not in **delegated legislation** made via **regulation**.
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
Case-study: Wyndham City Council

* In July 2012, an elderly man was attacked by a dog in a park and was hospitalised for his injuries.

* The owner of the dog was tracked down using metadata. The Council successfully prosecuted her.

TIA Act Annual Report 2013, p.53:

The Murder of Jill Meagher

“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.”

Ron Iddles, Secretary of the Victorian Police Association

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?
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:
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
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
A Chilling Effect on Freedom of the Press

“The data retention bill will compound these existing risks [to sources and journalists], and further enhance the chilling effect of government sources who may be considering speaking out on matters of public interest.”

- Paul Farrell, The Guardian

http://www.theguardian.com/media/2015/mar/01/deal-to-pass-data-retention-package-leaves-journalists-and-sources-exposed
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.
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.
Court of Justice of the European Union (CJEU) on Data Retention

In the European Union, mandatory data retention was struck down

Case: Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources [2014] All ER (D) 66 (April)

The CJEU said that the data retention law in place for all the European Union countries was excessive and interfered with the right to privacy under EU law.

See: http://online.wsj.com/news/articles/SB10001424052702304640104579488852878129392
United Kingdom

- **DRIP - Data Retention and Investigatory Powers Bill (UK)**

- Cabinet reshuffle, and emergency sitting of the UK Parliament to pass DRIP

- DRIP reintroduces powers which allow law enforcement to access telecommunications data without a warrant

Is this an attempt to limit debate about the data retention and surveillance powers?

See: http://www.bbc.co.uk/news/uk-28305309
FURTHER READING ON DATA RETENTION AND CHANGES TO TELECOMMUNICATIONS INTERCEPTION


- 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=c7f7c00b-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=4a7c3aee-1a1c-44e2-a806-28fb25a5be1d&subId=251942