Australia's Mandatory Data Retention Laws – Necessary national security measure or unreasonable intrusion of privacy?

A/PROFESSOR NILOUFER SELVADURAI

MACQUARIE UNIVERSITY

SYDNEY, AUSTRALIA

Introducing data retention laws

- What are data retention laws (DRLs)?
- Where have they been implemented?
- *Australia – Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015.
- *European Union – Data Retention Directive* 2006/24/EC. 2006] OJ L 105/54.
- Court of Justice of the European Union – *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesreg*ierung [2014] OJ C 175/6, [33-35].

Public policy justifications for DRL

- New and escalating threats of internet facilitated crime and terrorism.

- Increased ability of telecommunications systems to provide critical intelligence that can pre-emptively interfere and stop planned terrorist attacks and crimes.

- Current debate engendered by Apple's refusal to allow access by FBI to encrypted iPhones.

The new Australian laws

- *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015.
- Amends the *Telecommunications (Interception and Access) Act* 1979.
- Providers of relevant telecommunications services are required to retain telecommunications data associated with a communication specified in the Act for a period of two years.
- Arguably, now Australia has the most evasive DRLs amongst democratic industrialised nations.

Services subject to regulation

Mandatory data collection and retention obligations are imposed on:

- Services for carrying communications by guided or unguided electromagnetic energy.
- Services that enable communications to be carried by guided or unguided electromagnetic energy.
- Services operated by a telecommunications Carrier or an Internet Service Provider.
- Parties operating a service that **owns or operates infrastructure in Australia** that is used in the provision of any such service.

The data to be collected and retained

- Section 187C – Providers of relevant telecommunications services are required to retain telecommunications data associated with a communication specified in subsection 187AA for a period of two years.

- Section 187AA:
  - Categories of regulated information.
  - Categories of information outside ambit of laws.
  - Technologically-neutral drafting

Data security concerns

- Presently adopted safeguards
  - Encryption
  - Protection from unauthorised access
- However absence of clear minimum standard of protection to be maintained
- Continuing security concerns

Privacy concerns

- Continuing concerns as to proportionality of laws as scheme creates obligation to store data, falling within the relevant categories, for every Australian citizen.

- Act does not regulate content data but absence of definition of "content data" undermines this protection.

- Additionally, no prescriptions as to the basis upon which non-law enforcement agencies can access data.

The Decision of the European Court of Justice

- *European Union – Data Retention Directive* 2006/24/EC. 2006] OJ L 105/54.

- The CJEU found that the *Directive* infringed Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union: [2012] C 326/02.

- Which approach is preferable, that of Europe or Australia?

Reconciling the tension between competing interests

- Competing interests of national security and privacy.
- What is the proper balance.
- Comparing the EU and Australian approaches.

The new paradigm of discourse

- Harnessing technological advances to our advantage.

- Strategies for simultaneously strengthening both national security and privacy through encryption, creation of secure networks and other technological means
- The current state of discourse.