Public Wi-Fi provision: what are the privacy implications?

Ian McShane
Centre for Urban Research
RMIT University, Melbourne

RMIT UNIVERSITY

Privacy and public Wi-Fi: key points

- Telecommunications are subject to Australian Privacy Principles (APP) regulating the collection, handling, use and accuracy of personal information.
- APPs apply to public and private sector organisations *and* to third parties (eg cloud storage) wherever located.
- Privacy frameworks seek to regulate cross-border information flows and data storage.
- The definition of personal information may encompass metadata.
- New privacy standards are influencing business strategy & device design.
- Public Wi-Fi provision should adopt a ‘privacy by design’ stance.

RMIT UNIVERSITY

Privacy in Australia – key developments

- *Privacy Act 1988*
  - Focussed on public agencies
  - International influences; cross-border information flows; new forms of data processing
  - Introduced IPPs for public sector
  - Established privacy commissioner HREOC
- *Privacy Amendment (Private Sector) Act 2000*
  - Introduced NPPs for private sector (where no approved privacy code is in place)
- Australian Law Reform Commission: *For Your Information*, 2008
- *Privacy Amendment (Enhancing Privacy Protection) Act 2012*
  - Unified NPPs and IPPs into APPs, applying to public & private sector
  - Tightened rules on disclosure of personal information beyond Australian borders
  - Addressed use of personal information in direct marketing
  - Introduced stronger rules around data quality & protection.

RMIT UNIVERSITY

Privacy in Victoria

- *Privacy and Data Protection Act 2014 (Vict)*
  - Collection and handling of personal information in the Victorian public sector, including statutory bodies and local councils
  - Captures contracted service providers

➢ **Personal information**: “Information or an opinion…that is recorded in any form...about an individual whose identity is apparent, or can reasonably be ascertained...” (Part 3, PDPA Act)

RMIT UNIVERSITY

Telcos and privacy

- Industry codes prevailed before the *Privacy Amendment Act 2000*
- Covered by *Telecommunications Act 1997* and privacy legislation
- Carriers and carriage service providers are (likely to be) APP entities
  - 3rd parties (eg cloud storage) are required to comply with APPs wherever located.
  - Harmonises with EU General Data Protection Regulation (GDPR)
  - Subject to *Telecommunications (Interception and Access) Amendment Act (Data Retention) 2015*

RMIT UNIVERSITY

Is metadata personal information?

Google Street View project 2008 -2010

- Google found to have breached the *Privacy Act 1988* in surreptitiously harvesting 'payload' data (content) while photographing for Street View. (APC own motion, 2010)
- Other national jurisdictions found the 'header' data (SSID, MAC address, signal strength) constitutes personal information

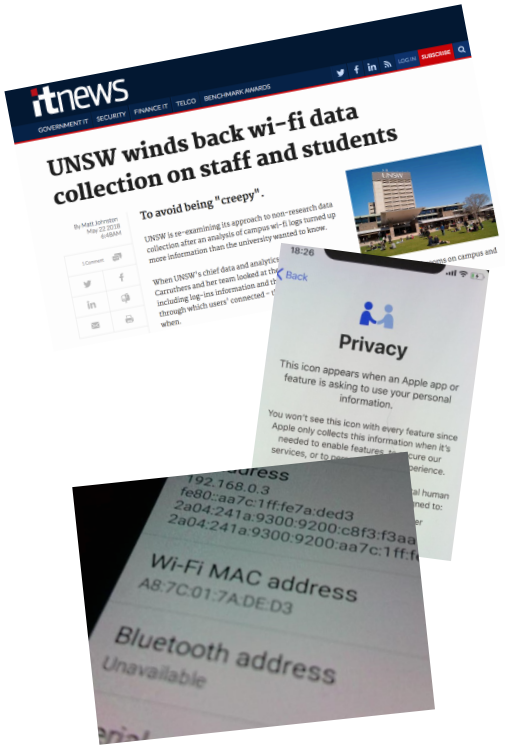
Ben Grubb v Telstra Corporation

- Data retained under TIA Act (s187LA) deemed to be personal information
- Privacy Commissioner found that Telstra contravened the Privacy Act 1988 by not providing Grubb with metadata (Grubb v Telstra [2015] AICmr 35).
- Telstra appealed successfully to AAT, and defended its position in Federal Court (Privacy Commissioner v Telstra [2017] FCAFC4)

RMIT UNIVERSITY

Privacy 2.0?

- Backlash against enterprise and government data leaks, over-reach
- Agencies, manufacturers are adjusting strategies and device designs
  - Apple's 'differential privacy', IBM's privacy pledge, MAC randomisation
- What are the implications for public Wi-Fi & urban analytics?



RMIT UNIVERSITY

A user perspective

- The privacy paradox: there is a mismatch between views on privacy and on-line behaviour
  - 10 million Australians regularly access public Wi-Fi
  - 2 million users transmitting financial & personal information on unsecured networks)
  - I million users log into work services without specific security measures
- Should users bear all risks? Do your terms and conditions prioritise user education, or risk and liability?

RMIT UNIVERSITY

GDPR as a benchmark?

The European Union's General Data Protection Regime (GDPR) applies to

- Entities outside the EU processing EU citizen data
- Entities within EU processing non-EU data

GDPR principles

- More explicit consent
- Right to explanation re auto profiling
- Right to be forgotten
- Privacy by design: emphasis on the data life-cycle – collection, storage, use, disposal.

RMIT UNIVERSITY