Ethics and Law of Privacy in the Digital Age & the Current Issue of Crypto-Crippling

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor, UNSW Law

Visiting Professor, Computer Science, ANU

http://www.rogerclarke.com/DV/DAP18 {.html, .pdf}

National Science Week

MOD, Adelaide – 2 August 2018

Ethics and Law of Privacy in the Digital Age
Current Technological Challenges

- Drones
- Autonomous Vehicles
- Visual Surveillance
- 'Facial Recognition'
- Biometrics Generally
- Genetic Data
- Big Data
- Open Data
- Analytics
- AI/ML, Neural Nets
- ...

- Data Expropriation
- Data Exploitation
- Transparency
- Automated Decisions
- Automated Actions
- Unfair Discrimination
- Accountability
- Recourse
- ...

What about the Privacy Act?

- Public Sector provisions of 1988 have been gutted
- Private Sector provisions of 2000 were written by the private sector, for the private sector

Exemptions and Exceptions in the Privacy Act as at December 2016

s.6A - Fully Exempted Activities
- archival evaluation
  http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6a.html
- **act or practice outside Australia**
  http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6a.html
- **act of practice required by an applicable law of a foreign country** (also s. 13D)
  http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6a.html

s.7 - Fully Exempted Entities
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s7.html
- FOI Act Schedule 1 (3 courts)
- FOI Act Schedule 2 Part I Div I (9 agencies)
- FOI Act Schedule 2 Part II Div I (3 agencies)
- a federal court
- a Minister
- several Commissioners or Commissions
- in relation to a record that has originated with, or has been received from [list of intelligence and similar agencies]

s.7B - Fully Exempted Activities
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s7b.html
- **Individuals in non-business capacity**
- **Employee records**
- **Journalism by a media organisation (minor condition re 'standards')**
- **Organisation acting under State contract**

s.7C - Political Acts and Practices
- Members of a Parliament etc.
- Contractors for political representatives etc.
- Subcontractors ...
- Volunteers ...

s.12A - State banking or insurance within that State

s.13B - disclosures to related bodies corporate

s.13C - transfer of data from a partnership to a successor partnership

s.13D - act of practice required by an applicable law of a foreign country (also s.6A)

s.16 - personal data held for Personal, family or household affairs

s.16A - Substantial Exemption for Permitted General Situations
- emergency: impracticable to gain consent and serious threat to life ...
- **protection of own legal interests: reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities**
- missing persons: to assist any APP entity, body or person to locate a person who has been reported as missing
- **protection of (any entity's?) legal interests: the establishment, exercise or defence of a legal or equitable claim**
- **resolution processes for (any?) dispute: for the purposes of a confidential alternative dispute resolution process**
- **diplomatic or consular functions or activities**
- **for war, peacekeeping or civil emergency outside Australia**

s.16B - Substantial Exemption for Permitted Health Situations
- **to provide a health service to the individual**
- **research relevant to public health or public safety**
- **the compilation or analysis of statistics relevant to public health or public safety**
- **the management, funding or monitoring of a health service**
- **third party's genetic data re health of genetic relatives**
- **patient incapable of giving consent**

s.20A – Credit Reporting
- **The Australian Privacy Principles do not apply to a credit reporting body ...**

s.20C – Credit Reporting
- **Authorisation of non-consensual disclosure and use of personal data for credit reporting ...**

s.72 - Public Interest Determinations
- the Commissioner is satisfied that the public interest in an act or practice substantially outweighs the public interest in adhering to that code or principle

s.80A - Temporary public interest determinations
- **As fo s.72 plus the issues require an urgent decision**

s.80G - Emergencies (see also ss.80P, 80Q)
- for a purpose that directly relates to the Commonwealth's response to an emergency or disaster in respect of which an emergency declaration is in force, incl.
- identifying individuals injured, missing, dead or involved
- assisting such individuals
- assisting law enforcement
- informing 'responsible persons' for such individuals

s.95 - Medical Research [enormous power granted to the NH&MRC]

s.95A - Health Information [enormous power granted to the NH&MRC]
- **research**
- **the compilation or analysis of statistics, relevant to public health or public safety**

s.95AA - Genetic Information [enormous power granted to the NH&MRC]
- **lessening or preventing a serious threat to the life, health or safety of an individual who is a genetic relative of the individual to whom the genetic information relates**

s.100 - Regulations, incl.
- **necessary or convenient for carrying out or giving effect to this Act**

Amendments 1989-2018 have bloated the Act to 78,000 words

Definitions

Defined outside the Privacy Act? Not at all?
- body corporate

s.6 Definitions
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html
- agency
- APP entity
- corporation
- employee record
- enforcement body (7 Clth agencies named, but highly extensive; all State and Territory "police force or services"; corruption bodies; but enormously extensive; and extensible by Regulations as well)
- media organisation
- non-profit organisation

s.6A
- breach

s.6C Definitions
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6c.html
- organisation

s.6D Definitions
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6d.html
- small business
- small business operator

s.13
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s13.html?stem=0&synonyms=terference%20with%20the%20privacy%20of%20an%20individual
- an interference with the privacy of an individual

s.16A
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s16a.html
- permitted general situation

s.16B
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s16b.html
- permitted health situation

s.80G - emergencies
- permitted purpose

s.80P - emergencies
- designated secrecy provision

APP8.1
- overseas recipient

Exceptions and Exemptions in the APPs as at December 2016:

http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html

APP2.2 – anonymity and pseudonymity
- if the APP entity is required or authorised to deal with individuals who have identified themselves
- if it is impracticable

APP3 – collection of solicited personal information
- consent and reasonably necessary for, or directly related to, one or more of the agency's functions or activities
- consent and reasonably necessary for one or more of the organisation's functions or activities
- required or authorised by law
- a permitted general situation exists
- a permitted health situation exists
- an enforcement body ...
- a non-profit organisation ...

APP6 – use or disclosure of personal information
- [Usual long list similar to APP3]

APP7 – Direct Marketing
- Despite the nominal prohibition, [Authorisation of non-consensual, opt-out use of personal data for direct marketing]
- Despite the nominal prohibition, [Authorisation of non-consensual use of personal data by contracted service providers for a Commonwealth contract]

APP8 – cross-border disclosure of personal information
- [even longer list of loopholes]

APP9 – adoption, use or disclosure of government related identifiers
- [Usual long list similar to APP3]
- any organisation can be authorised by Regulation

APP10 – quality of personal information
- ... such steps (if any) as are reasonable in the circumstances ...

APP11 – security of personal information [and destruction]
- ... such steps (if any) as are reasonable in the circumstances ...

APP12 – access to personal information
- agencies retain the scope to use all FOI and other exemptions
- organisations have a long list of loopholes available
- ... give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so
- organisation may charge a fee

APP13 – correction of personal information
- ... such steps (if any) as are reasonable in the circumstances ...

The APPs have bloated to 5500 words incl. 27 instances of "reasonable"

What about the Privacy Act?

- Public Sector provisions of 1988 have been gutted
- Private Sector provisions of 2000 were written by the private sector, for the private sector
- OAIC / PC'er protects them, not us
- OAIC crippled by bureaucracy, under-resourcing

itnews

OAIC limps on

No details on privacy, FOI commissioner roles.

What about the Privacy Act?

- Public Sector provisions of 1988 have been gutted
- Private Sector provisions of 2000 were written by the private sector, for the private sector
- OAIC / PC'er protects them, not us
- OAIC crippled by bureaucracy, under-resourcing
- 'Open Data' mission is to remove safeguards
- A new Data Commissioner whose function is to trump the Info and Privacy Commissioner(s)
- ABS MADIP Program consolidates personal data

Open data: Government to establish a 'National Data Commissioner'

Unveils $65 million push to make more government data available

Rohan Pearce (Computerworld)
01 May, 2018 10:50

Multi-Agency Data Integration Project (MADIP)

The Multi-Agency Data Integration Project (MADIP) is a partnership among Australian Government agencies to combine information on healthcare, education, government payments, personal income tax, and the Census to create a comprehensive picture of Australia over time.

What about a Privacy Tort?

LRCs recommended
Labor Govt floated
Murdoch vetoed

APF Policy Statement
https://privacy.org.au/policies/right-of-action/

Clarke R. 'Media Paranoia Distorting Facts on Privacy Tort' Crikey, 1 August 2011

Sir Cliff celebrated his victory over the BBC (Image: PA)

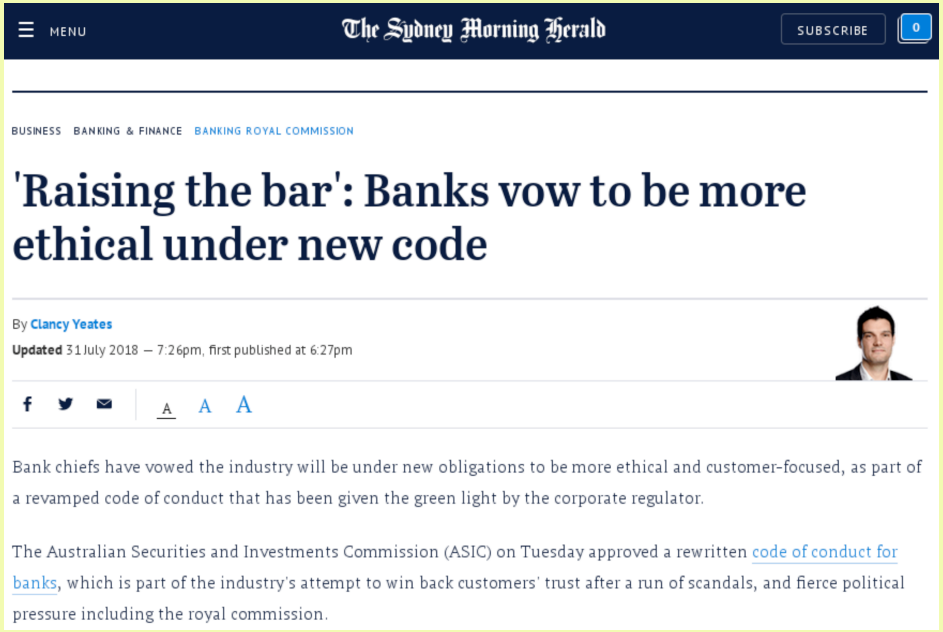
Greater Threats, so Better Safeguards are Needed

- **Data Privacy**
  Vast quantities of data 'born digital' or digitised; Data silos broken down; Wide availability of pseudo-anonymised (actually re-identifiable) data
- **Communications Privacy**
  Most messages are now sent electronically, and intercepted and accessed, even ephemera recorded
- **Behavioural Privacy**
  Electronic surveillance, plus visual surveillance by means of chip-cards, biometrics, CCTV, ANPR, ...
- **Experiential Privacy**
  Once-anonymous reading, buying, borrowing, viewing, watching is now all in identified form

Can Ethics Help?

Can Ethics Help?

- Ethics offers intellectually stimulating discussion
- Ethics supports *ex post facto* analysis, e.g. of systematic misbehaviour by the big banks



MENU The Sydney Morning Herald SUBSCRIBE 0

BUSINESS BANKING & FINANCE BANKING ROYAL COMMISSION

'Raising the bar': Banks vow to be more ethical under new code

By Clancy Yeates

Updated 31 July 2018 — 7:26pm, first published at 6:27pm

A A A

Bank chiefs have vowed the industry will be under new obligations to be more ethical and customer-focused, as part of a revamped code of conduct that has been given the green light by the corporate regulator.

The Australian Securities and Investments Commission (ASIC) on Tuesday approved a rewritten code of conduct for banks, which is part of the industry's attempt to win back customers' trust after a run of scandals, and fierce political pressure including the royal commission.

Deep moral turpitude and illegal behaviour defused by an unenforceable 'Code'

Can Ethics Help?

- Ethics offers intellectually stimulating discussion
- Ethics supports *ex post facto* analysis, e.g. of systematic misbehaviour by the big banks
- Ethics embodies every complexity and contradiction that smart people can dream up
- Ethics enables prevarication
- Ethics provides endless excuses for inaction

Can Ethics Help?

NO

But pragmatic, instrumentalist techniques can
e.g. Technology Assessment, Privacy Impact Assessment

Assessment Categories

Organisational Focus
- Business Case Formation
- Security Impact, aka Threat Risk Assessment (TRA)

Technology Focus
- Technology Assessment (TA)

Social Impact Focus
- Rights IA
- Ethical IA
- Surveillance IA
- **Privacy Impact Assessment**
- Data Privacy IA

Compliance Focus
- Regulatory Compliance
  - Org'l Self-Regulation
  - Industry Self-Regulation
  - Co-Regulation
  - Formal Regulation
- Privacy Law Compliance
  - All Statutes, Delegated Legislation, Common Law
- Data Protection Law Compliance
  - An EU Directive, a Statute

Privacy Impact Assessment: Its Origins and Development
http://www.rogerclarke.com/DV/PIAHist-08.html

Enhancement of Legal Protections?

- Parliaments are merely bear-pits

- Political priorities are driven by (a) funders and (b) opinion polls and focus groups
- Public servants serve their own needs, not people's
- Privacy is perceived as an impediment to business, government, and the sacred cow, 'national security'

Organisational Protections?

- Isn't privacy a strategic factor for organisations? Unfortunately, they don't perceive it to be so
- **'Privacy doesn't matter, until it does'**
- Companies blunder from one misconceived design to the next media disaster and data breach
- Meaningless media releases are seen as the means to minimise financial and reputational harm

Privacy and Dataveillance, and Organisational Strategy
http://rogerclarke.com/DV/PStrat.html (**1996**)

Make Privacy a Strategic Factor - The Why and the How
http://rogerclarke.com/DV/APBD-0609.html (**2006**)

Vignettes of Corporate Privacy Disasters
http://rogerclarke.com/DV/PrivCorp.html (2006-18)

Facebook stock suffers largest one-day drop in history, shedding $119 billion

The company's shares plunged almost 19 percent,

Investors were spooked by Facebook's forecast showing that its number of active users is growing less quickly than expected, while the company also took a hit from Europe's new privacy laws.

The share collapse merely returned Facebook shares to a level last seen in early May, a sign of just how bullish investor expectations had been running. At that time, the stock was still recovering from an earlier battering over a major privacy scandal.

"The implementation of GDPR gave a large number of Facebook users control over their privacy, and it should have been patently obvious to investors (and to us) that allowing users control would result in slightly lower engagement," he noted, alluding to Europe's General Data Protection Regulation privacy rules.

CBS News, 26 Jul 2018

Technological Protections?

- Individual technology-developers are diverse
- Some have developed privacy-friendly tools (PETs)

PITs and PETs

- **PITs** – Privacy-Invasive Technologies
- **PETs** – Privacy-Enhancing Technologies
  A long line of work since 1995
  - **Counter-PITs**, **incl. crypto-protections** for data in storage, in transit; authentication, ...
  - **Savage PETs**
    for Persistent Anonymity
    incl. crypto-protections
  - **Gentle PETs**
    for Protected Pseudonymity, and hence accountability as well as freedom

Technological Protections?

- Individual Technology-Developers are diverse
- Some have developed privacy-friendly tools (PETs)

- Very few PETs have achieved widespread adoption
  (Exceptions: SSL/TLS = https, anti-virus tools)
- The Business Verdict: PETs are 'Mostly Harmless'

- **Corporations embed Privacy-Invasive Technologies**

How does all this apply to Cryptography?

- **Telcos must assist LEAs even in minor matters**:
  "pecuniary penalties" (fines, nomatter how small)
  "protecting the public revenue" (any investigation)
- **Telcos and ISPs must provide data to agencies**
  Telecommunications Act ss. 311-316
- From 2018, Telcos must now divulge **details of architecture, infrastructure designs, technologies**, and submit to instructions about them from LEAs
  Amendments in Telecomms and Other Legislation Amendment Act 2017
- An emergent Bill is to (magically) enable **access to cryptographically protected data and messages**
  "an [unexplained] obligation to assist agencies with decryption"

APF's Meta-Principles for Privacy Protection

https://privacy.org.au/policies/meta-principles/

1. Evaluation
2. Consultation
3. Transparency
4. Justification
5. Proportionality
6. Mitigation
7. Safeguards
8. Audit