Uberveillance

Ubiquitous online surveillance and computer science – ethical and legal issues

David Vaile
Co-convenor, Cyberspace Law and Policy Community
UNSW Faculty of Law
http://www.cyberlawcentre.org/it_ethics_and_law/

For UNSW CSE – IT Law and Ethics – September 2014

Outline

1. Risks of personal information used for other purpose
2. What are the programs Snowden revealed
3. US Legal issues, UK issues
4. Australian issues
5. Google, Facebook and social media privacy? (move fast)
6. IT security undermined
7. Data Sovereignty and cloud
8. Whistleblowers and leakers
9. Big Data and predictive analytics
10. Panopticon and chilling effect

Intro

Important to not pre-judge issues

Evidence and facts are critical

Spin is used to obfuscate both technical and legal issues

There are justifications for some uses of this tech

But people have fought for hundreds of years to avoid oppression by the state/government and businesses

Questions about proper levels of oversight, proper uses of technology, proper restraints, oversight

Most important – identify the issues, and the strength of evidence

Open-ness cannot be complete, but is the foundation of the system we are protecting – how far can secrecy help?

Programs Snowden revealed?

- Phone
- ‘metadata’
- Email
- Fibre
- Security backdoors
- Cooperation with ISPs, ICHs
- Sharing with 5 Eyes, Israel, Germany…
- Retention, targeting of encrypted comms

US legal issues?

- 4th Amendment Constitution: warrant, suspiciion
- Legal basis: FISA, Patriot Act
- (Data Sovereignty report)
- Oversight by FISA court - anomalies
- "US person" – jurisdiction split with agencies
- Executive oversight?
- Legislative oversight?

UK issues

- Lack of 1st Amendment US Constitution: 'prior restraint' on publication
- Legal basis: vaguer?
- GCHQ – outsourcing some tasks illegal for NSA?
- Extent of activities in the EU?
- Recent knee-jerk RIPA law, bypasses ECJ ruling that the EU Data Retention Directive is invalid (didn't work either)

Australian issues

- Data Retention plan: back in the news
- Legal basis: vague? No right to privacy, no constitutional rights?
- ASD etc – outsourcing some tasks illegal for NSA?
- 5 Eyes roles?
- Telecommunications Act s313? 'Prevention'?
- Lack of transparency & policy governance?

s 313 TA and pre-crime, blocking

- s 313 *Telecommunications Act 1997* (Cth) creates 2 ISP obligations:
  313(1) 'do your best' re Crime Prevention,
  313(3) 'reasonable help' for law enforcemnt (interception etc.)
- Confusion: no obvious power for any body to require you to do anything in 313(1) prevention, but you must help collect evidence for prosecution of specific offence (law enforcement)
- Crime Prevention: open ended, no evidence, no limits 'pre-crime'
  Law Enforcement: strong powers but strictly targeted, evidence.
- Preparatory and 'inchoate' offences bridge the gap, bad trend...
- Danger in creating an expectation that ISPs/CSPs have open obligation to do whatever anyone says to make Internet about CP
- Easy for ISPs to just do what is asked, even tho 313(1) requires 0
- Lack of transparency, reporting, oversight, governance, proportion?

Google, Facebook & social media privacy?

- Active cooperation
- Similar instincts
- Encourage people not to care of consequences
- Hidden or suppressed roles
- Honeypots
- Contradictions: new DDoS protection?
- Masters of spin: 'Don't be evil', 'share'

‘Move Fast and Break Things’

- ‘See what you can get away with’/
  ‘We’ve not been caught [yet]’
- ‘Ask Forgiveness not Permission’ (Cobol guru)
- Disposable Prototyping, not Compliance
- What works for software does not work for personal or critical information
- Your secrets are not revocable, disposable
- Not about compliance – assumes risk is neglible – assumes others carry the risk!
- Cult of Disruption: avoid tax, rent, wages,

So, what's the blind spot of the smartest guys in the room?

- Online social networking giants are intensely creative software and advertising powerhouses, driven by hacker instincts, now massive.
- **'Move fast and break** [take?] **things', 'Ask forgiveness not permission':** slogans from immature software developers raised to think throwaway prototypes, not compliance and risk.
- Risk projection
- Category error: human personal information, the stuff of lives, is **NOT disposable**. 'Oops, we'll fix it next version!' is not an answer when personal information abuse causes irrevocable harm. Their governance model, based on rapid prototyping, cannot cope.
- These models are now so profitable that there is now great commercial pressure to NOT adapt to this hard and real truth.

IT security, crypto undermined

- Back doors
- NIST standards
- TOR
- Uncertainty for IT security industry
- "Security" agency undermines security?
- Security for whom? Anyone?
- Conflict between security role and spying role – governance fail?

Data Sovereignty and the Cloud

- Trust is critical
- SWIFT case
- Backlash
- Germany, Mexico, Brasil
- France, Sweden
- Cloud industries undermined?
- Geolocation of data?
- Data Sovereignty or Digital Protectionism?
- TPP, TTIP, CISA: Treaty says no, can't choose

Big Data and 'predictive analytics'

- Behavioural/psychographic profiling?
- Prescriptive analytics?
- Machine learning: start with no purpose
- Algorithms and data beyond human comprehension?
- Beyond review or error detection?
- OK for ads, not so much for drone strike
- The heart of autonomous weapons, or other self-directing intervention tools?

Big Data: Fun, but is it safe?

- Built by marketers Google (MapReduce), Facebook (data centres) for marketing purposes: slightly better ad targeting
  'Flavour of 2012'
- Fundamentally hostile assumptions for privacy, security, confidentiality: 'collect it all', forever, we'll find a reason...
- OECD Privacy Principles start from permitting PI use for a known purpose, for which it was collected, but not one big pot
- 'Association' not 'causation': is underlying sloppy logic on dirty data fit for human consumption, if the decisions are real?
- Reverses the presumption of privacy? Fails the Consent model? Encourages passive acceptance of ubiquitous, unregulated surveillance?

Whistleblowers and leakers

- Role as sysadmin:
- Snowden: very selective, via journos
- Manning/Wikileaks: indiscriminate?
- Glenn Greenwald: *The Intercept*
- Different views?
- Serious attacks on journalists and leakers, including AU journalists (proposed) and US journalists (actual)
- Allegations of treason, medals for human rights...
- Backlash against workers in security agencies: paranoia and suspicion about loyalty

Uberveillance After Snowden

- Edward Snowden enabled journalists to publish info about surveillance, because he felt NSA + 5 Eyes broke US Const 4th Amdt
- Warrantless, suspicionless mass surveillance on unprecedented scale; strange interpretations of loose laws, and Big Data scoops
- Triggers global debate about 'Proportionality' of online surveillance
- Justification: was foreign terrorists, but PCLOB and ECJ see no ev.?
- Metadata: mere number called, or "everything about someone"?
- US Mathematical Society: given NSA's attacks on security via NIST encryption randomness back door, is work for them unethical?

External risks of personal information used for an unintended purpose?

- OECD Privacy Principles (not US) focus on purpose
- Prospects for employment, insurance, housing, travel, security clearance, public office …
- Damage personal relationships, trust, family, marriage, sex …
- Sexual or other harassment, smearing, shaming, vilification
- ID theft, fraud, burglary, robbery, scams, framing
- Profiling as national security, criminal, or political risk; blackmail
- Recruitment into inappropriate activities by pressure
- Personalised messaging designed to 'go under the radar', use personal preferences to avoid critical assessment of message

Panopticon and chilling effect?

- Michel Foucault, *Discipline and Punisment: The Birth of the Prison* (1975)
- The prison in your head?
- Central guard tower with one way view, each cell's interior exposed
- Guard is not necessary?
- Consciousness of being watched changes your mind and your behaviour
- A conscious aim of great firewall of China: we know you know we know what you're up to
- *SF v Shoalhaven* [2013] NSWADT 94, CCTV case

Questions and Discussion

Thanks

David Vaile
Cyberspace Law and Policy Community
Faculty of Law, University of NSW
http://www.cyberlawcentre.org/
d.vaile@unsw.edu.au