Legal Perspectives on the Software Industry in a surveillance economy: Dataveillance

Ubiquitous online surveillance and computer science - ethical and legal issues

David Vaile
Privacy and Surveillance stream lead, Allens Hub for Technology, Law and Innovation, UNSW Faculty of Law
http://cyberlawcentre.org/comp4920/

https://flipboard.com/@unsecurity
Uberveillance

A. Outline for Intro law & ethics

- Strange bedfellows – Law and IT/Comp Sci
- About the Legal system
- Liability
- Software development – immature?
- 'Data Integrity Profession'?

Software, Law and Ethics

- Strange bedfellows: legal 'rules' are different
- How the law is made, and how it works
- Differing principles and standards
- 'Rule of Law', 'Natural Justice'

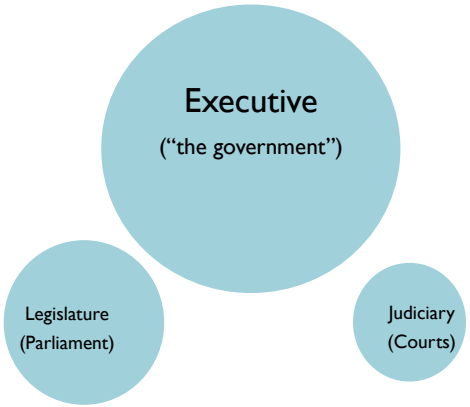
What shapes the law?

- Ongoing struggle between interests
- Commercial reality
- Technical reality
- Public standards
- International effects (indirect)

Features of the legal system

- Main divide: Criminal <-> the rest (civil)
- Criminal
  - Launched by state, trial, conviction or acquittal
- Civil
  - Sued by other party, damages, restitution
- Sources
  - **Statutes** ('Laws') set rules, **Cases** interpret (precedent)
  - **Jurisidiction**: which laws and courts? AU? US? EU?
  - **Contract** – private laws?
  - Codes, 'Code', convention
- Obligations: from Statutes and Contracts
- Everything is arguable, no right answer – reflexive

Three wings of government



Sources of law

	Example	Function
Statutes	'Laws' or Acts: *Copyright Act 1968*	Set general rules, in a jurisdiction
Legislature	NSW Parliament	Listen to submissions, change laws
Codes	ASMRO Privacy Code	Industry-specific clarification of general law
Jurisdiction	NSW, Cth	Whose laws and courts apply?
Court 'Cases'	*R v Usmanov*	Interpret laws in a dispute instance
Precedent	Case on same point	Critical in cases: must follow past
Contracts	Facebook Terms	Private agreement on terms
Norms, Conventions	Right to free speech	De facto constraints
'Code' (Lessig)	DRM	May prevent or allow outside law

What matters?

- Breaking the law? Liability
- Getting caught? Enforcement
- Losing your job? Professional
- Losing self respect? Ethics
- Or just building crap? Reputation

Rule of law

- No-one is above the law
- 'Separation of powers' (3 wings)
- Principles of 'Natural Justice'
- Decision of a court is binding
- Statutes interpreted by known principles
- Interests and arguments taken into account and balanced
- Restraint on arbitrary power (king, Trump)
- If you don't like it, change the law (legisl.)

'Natural Justice' - Fairness

Rights to:

- Know the case against you (evidence, logic)
- Make case, be heard before decision
- Test and bring evidence
- Impartiality, no bias, not corrupt
- Decision only on evidence and law
- Procedural review (appeal)

'Natural Justice' – tech fail?

Examples: App store or Facebook

- Don't know rules, case against you?
- Don't get heard before decision?
- Can't test and bring evidence?
- Partiality, bias, corrupt influence?
- Decision on unknown criteria, facts?
- No procedural review (appeal)?

Private, arbitrary, unilateral contract: help?!

Risk as a factor in design, ops

- Risk thinking is central in avoiding common big IT project fail
- Failure is necessary input to iterative development
- Lawyers interested when failures hit the fan
- Allocate responsibility for bad outcomes
- Intention and motive relevant ('I meant no harm')
- Real impact is central – Ignorance is no defence?
- But *Broadcasting Services Act 1992 (Cth)*, Sch 5 Cl 91: no liab.
- BSA: ICH is not responsible until **aware** of potential harm
- Disincentive to moderate, check, know of harm
- Rewards/mandates ignorance
- Immunity evaporates when you tell them

Risk (cont.)

- BSA assumes 'Forgiveness, not permission' model
- ICH don't check, user doesn't ask permission
- Assumes 'Take Downs' cure all ills
- Fine for software – disposable prototype
- But not for secrets, people: information risk fail
- Facebook Live streaming: misused for snuff, assault movies, too late to take down
- Conflict with the business model and culture of the 'Cult of Disruption':
- Legal immunity does not cure the risk, it makes it worse, tempts host to claim not responsible, and users too. What could go wrong?

Professional Liability

- Nature of Profession?
- Membership of Professional body
- Registration required to work?
- Self-regulation
- Insurance
- Peer attitudes
- Reputation

'Data Integrity Professionals'

- Law firm IT; medical informatics?
- A new profession?
- Certification, training curriculum
- Registration to work? Not sure…
- Self-regulation? Complaints? Exclusion?
- Body of expertise, identifiable expert
- Sensitive data, high ethical standards, expectations of data subjects
- Meet legal evidentiary criteria (forensics)
- Can manage others (IT security, analytics)

B. Outline for **Dataveillance** – Govt & Corp 'surveillance economy'

1. Why do I care – what this is about
2. What are the programs that Snowden revealed?
3. US and 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

What this is about

- Help you understand the complexity of debates on regulation of online surveillance
- Reasons for caring about privacy, personal info and IT security, confidentiality
- Critical view of governance and oversight
- Snowden 2013 revelations show the terrain
- Apple v FBI 2016 gets very specific
- My Health Record – current example
- Don't see it as black and white
- Topic is very political, manipulated, emotive

Why should I care?

- Projection of risks to data subjects?
- Panopticon/chilling effect?
- Undermines security for all?
- Defence and offence may not be compatible under one roof?
- Reasonable needs of LEAs/Nat Sec
- Militarisation of data space?

External risks of 'personal information' used for an unintended purpose?

- OECD Privacy Principles, GDPR (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

- Psychological impact of surveillance
- Often not taken into account enough
- *SF v Shoalhaven* CCTV case: this motive
- Information/knowledge is power
- One way/asymmetric visible observation
- Consciousness of being spied on
- Changes behaviour, thoughts, comms.
- Whither free speech, freedom of thought, freedom of association?
- Deliberate method of Chinese monitoring: self censorship is the goal, not catching everything

Approach

- 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 their own states and government
- 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?

Gov programs Snowden revealed?

- 'Collect it all' - NSA
- Phone, Email, 'metadata', content
- Fibre backbones
- Security backdoors, weak crypto (NIST)
- Cooperation with ISPs, ICHs
- Sharing with 5 Eyes, Israel, who else…
- Targeting other govts, commercial? (East Timor)
- Retention, targeting of encrypted
- Use for drone targeting in undeclared wars?

IT security undermined

- Back doors
- NIST standards
- TOR
- Uncertainty for IT security industry
- "Security" agency undermines security?
- Security for whom?
- Recent deprecation of strong crypto
- But top spies are split – some seem to recognise need for security, after all

Apple v FBI: scenario / arguments

- Apple
  - Not the main phone – low value
  - Only 20 minute gap
  - Apple assisted 10,000 iCloud accesses
  - Ruin our rep
- FBI
  - Under a warrant, not warrantless, suspicionless
  - Worst case, actual shooter, terror threat
  - 'Just this one time', one-off
  - Old iphone, old iOS, not a general issue

Apple v FBI 2016: issues

- Creation of a temporary back door
- Custom creation on request
- A special version of crackable OS
- Breach IT security of its own OS
- First of many? Test case?
- How would you resist after #1?
- Selective political choice: manipulation of debate? Or good example?

Data Sovereignty and the Cloud

- Law based on territorial jurisdiction
- Trust is critical
- SWIFT case
- Backlash
- Germany, Mexico, Brasil, France, Sweden
- Cloud industries undermined?
- TPP, TTIP, CISA : Data Sov. v "Digital Protectionism"? No, you can't choose
  - Local law and contracts overturned by ISD
- Control & location important: jurisdiction

EU legal issues

- GDPR 2018 applies to data about EU people, wherever the data is held
- GDPR De facto global standard because US tried to avoid regulation, failed to protect non-US persons
- See also July 2018 California Privacy Act – like GDPR
- Schrems I case, EU Court of Justice 2015 – end of the Safe Harbor fiction about the US Cloud
- Schrems 2011 complaint should have prevented Cambridge Analytica –
- UK Parliamentary committee July 2018 calls for end of impunity for Facebook in publication of fake news
- None of this protects Australians – we are left out

US legal issues?

- 4th Amdt Constitution: warrant, suspicion
- Legal basis: *FISA*, *Patriot Act*, ss 702, 215
- (*Data Sovereignty and the Cloud* report)
- Oversight by FIS court – anomalies?
- "US person:" jurisdiction split w. agencies
- Executive oversight? Legislative oversight?
- PCLOB reports: one invalid, other valid
- Little or no evidence of effectiveness alone
- Recent Congressional cancel one, rest++

UK issues

- Lack of 1st Amendment US Constitution: 'prior restraint' on publication
- Legal basis: vaguer?
- GCHQ – outsourcing tasks illegal for NSA?
- Extent of activities in the EU?
- ECJ – Data Retention Directive invalid
- Many countries pull back
- RIPA law 2015: Deep review. Double down.
- 2016: attack on E2E Crypto
- 2018: inquiry into Facebook andf 'fake news' attacks, effects on Brexit, move to regulate

Australian issues

- Data Retention law: mass surveillance
- IP v4 exhaustion, CG-NAT, 30K samples?
- Legal basis: vaguer?
- ASD etc – outsourcing tasks illegal for NSA?
- '5-Eyes' role
- Telecommunications Act s313?
- Lack of transparency?
- 'Proportionality': how balance 'security' cf. privacy, PI security, confidentiality?
- Plan to undermine encryption, dispute over 'back doors'

Google, Facebook & social media privacy?

- Active cooperation with spooks? Reconsidered?
- Similar instincts – collect it all
- Encourage people not to care of consequences
- Hidden or suppressed roles
- Honeypots
- Contradictions: new DDoS protection?
- Masters of spin – Cult of Disruption
- (Apple different? Recent crypto update...)
- Cambridge Analytica, AI, targeted intrusion on democratic process?

'Move Fast and Break Things'

- Facebook motto up to 2014
- 'See what you can get away with'
- 'See if you get caught'/
  'Ask Forgiveness, not Permission' (Grace Hopper)
- 'We haven't been caught [yet]'
- Disposable Prototyping, not Compliance with rights
- BUT: what works for **software** does not work for **personal** or critical information
- Your secrets are not revocable, disposable
- Not about compliance – assumes risk is negligible – assumes others carry the risk!
- Version 2.0 does not fix someone's life after breach

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 things', 'Forgiveness not permission':** slogans from software developers raised to think throwaway prototypes, not compliance and risk.
- Risk projection onto others?
- 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.

FB and Cambridge Analytica

- Schrems complaint 2011, audit 2012
- Irish DP and FB fotzed until 2015, door open
- Kogan 2014 app, 'experiment', 'licenced'?
- CA obtained Kogan's data, used to intervene in US election to support Trump
- First potential instance: psychographic profiling from FB helping elect questionable candidate
- FB in denial, refuses to accept editorial role despite having captured the news role
- No fact checking, open to misinformation
- If you influence an election, you influence laws, judicial appointments, who gets to be government – YUGE!!!

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 & 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?

Privacy

- 'Right to be left alone'
- Defeat of Australia Card 1986, *Privacy Act*
- Limited rights of data subjects
- Restricts what technology can do
- Requires IT security, data integrity
- Affects everyone
- Weaker laws in AU *cf.* other countries?
- Weaker enforcement? No right to sue
- Now includes breach notification

Definitions are critical: IP = 'PI'?

- Legal regulation based on precise specification of scope of key terms.
- Definitions are often the centre of court cases
- Inclusion in category determines how law applies
- Example: is an IP address 'personal information' (PI)?
- In privacy law in Australia, key term is PI
  - EU: 'Personal data' (PD) – similar
  - US: 'Personally Identifiable Information' (PII) - narrower
- Varies from jurisdiction
- Varies with precise legal definition, context

Definitions are critical: IP = 'PI'? /2

- Grubb: *Telstra v Privacy Commr &ors* 2016 FC
- Grubb wanted his metadata
- Telstra said not metadata
- Commissioner said yes
- Court said no
- But has limited legal precedent value:
  - S 187LA of *Telecommunications Act 1997* (Cth) says metadata including IP?) is PI for metadata retention purposes
  - New version of PI definition came into force 2014, after the facts of this case, so the case refers to obsolete legislative definition
- If IP is PI, then everyone should have many more protections – the metadata retention scheme assumes this is not really sensitive.

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 lake
- 'Association' not 'causation': is underlying sloppy logic on dirty data fit for human consumption, if the decisions are serious?
- Reverses the presumption of privacy?
- Fails the Consent model? Encourages passive acceptance of ubiquitous, unregulated surveillance?

Big Data and predictive analytics

- Big Data: marketing buzz word. Decontrol
- "Fishing expedition" in Data Lake
- Threat: silo security/privacy, control by purpose
- Machine learning: start with no purpose?
- Reluctance to accept predictions flawed?
- 'Prescriptive analytics'?
- Potential for discrimination
- Legal responsibility requires causation; data usually gives correlation
- Algorithms and data beyond human comprehension?
- Beyond review or error detection?
- OK for ads, but drone strike 'ruins your day'.

‘Open Data’

- If not personal info, no issue, a good thing
- Recent UN consultation last week:
- Exclude unit level record from personal information from ‘Open Data’ publication
- Governments reluctant to do this
- De-identification said to be enough to make the data no longer PI
- But Re-identification risks grow constantly: machine learning, proliferation of other data
- No audit, no remedy if data is re-identified
- Projection of risk onto data subject?

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
https://flipboard.com/@unsecurity
Uberveillance

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?