Dataveillance Law:
Modalities, Categories and Examples

Roger Clarke and Graham Greenleaf

Xamax, UNSW Law, ANU RSCS, APF and UNSW Law, APF, AustLII

5th Asian Privacy Scholars Network Conference, Auckland, Dec. 2016

Roger.Clarke@xamax.com.au, graham@austlii.edu.au

The Concept of 'Dataveillance'

- First defined as ***systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*** (Clarke 1988)
  - focus on information systems that have monitoring of individuals as a significant function
  - distinguished mass from individual dataveillance
- 30 years later, a broader definition is needed: ***systematic DATA COLLECTION AND/OR use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons***
  - adding collection for surveillance & later use

Forms of Regulation of Dataveillance

Dataveillance can be regulated (per Lessig) by:

1 Law – defined here as 'dataveillance law'

2 Markets (costs/benefits of surveillance; over-intrusion leads to loss of customers)

3 Ethics/custom (professional codes; 'creepiness')

4 'Code' / 'architecture' (encryption; default settings)

Other candidate forms of regulation:

5 'Feedback' (adverse/positive comments regulate)

6 Surveillance per se (known surveillance regulates)

Scope of 'Dataveillance Law'

1. **Law made by the State** (incl. treaties, legislation – primary & delegated, court/tribunal decisions)
   - Incl. 'meta-regulation' (Parker, 2007) the regulatee is merely required to satisfy some broad principle(s)
     - e.g. *Privacy Act* s.78(4), "a media organisation is exempt ... if ... [it] is publicly committed to observe standards that ... deal with privacy ... and ... have been published"
2. **Law made by Private Entities**, enforced by the state
   - incl. contracts; some co-regulation; binding self-regulation (?)
3. **Quasi-Legal Instruments that are customarily observed**
   - MOUs between local/international enforcement bodies
   - Guidelines by oversight agencies
   - Industry self-regulation
   - Corporate governance

Defining 'Dataveillance Law'

- In full: Dataveillance law comprises
  the set of formal regulatory mechanisms that:
  - mandate, authorise or prohibit organisations (conditionally or unconditionally)
  - to or from using specific surveillance mechanisms
  - in relation to one or more persons; and
  - involve identifiable recorded data
- Briefly put: Dataveillance law comprises regulatory mechanisms that affect the practice of surveillance (monitoring or investigation) involving data about people

*This concept is (surprisingly) novel in the surveillance and privacy literatures – there are no attempts to explain the relationship(s) between **law** and data surveillance*

Six Modalities of Dataveillance Law

1 **Mandatory** (cf. Necessary) – Laws formally requiring organisations (public or private sector) to carry out particular DV activities

2 **Permitted** (cf. Possible) – Laws providing formal permission for DV activities (negating possible claims of illegality), or providing capacity to organisations to do so, but not making it mandatory to do so

3 **Conditionally Permitted** (cf. Contingent possible) – Laws permitting DV activities to occur, subject to conditions on occurrence, or constraints on operation, which must be satisfied

4 **Unregulated** – No relevant law either permitting or prohibiting

5 **Conditionally Prohibited** (cf. Contingent proscribed) – Laws prohibiting DV activities unless particular tests are satisfied

6 **Prohibited** (cf. Proscribed) – Laws formally prohibiting organisations from carrying out particular DV activities

‘Data Protection’ Acts –
Where do they fit as dataveillance laws?

- They demonstrate that legislation rarely fits in only one of the 6 modes, because most overlap 2 or more modes
- Their ostensible role is **prohibition** or **imposition of qualifying conditions or safeguards** on DV. **<u>But</u>**:
  - They rarely explicitly proscribe a DV activity (M6)
  - Prohibitions are subject to exceptions (M5)
  - It is common to impose conditions (M3)
- **<u>And</u>** they have a major role in **formally permitting** previously questionable DV activities (M2), or **permitting them subject to conditions** (M3)
  - That shifts such DV activities from M4 to M2 or M3
    e.g. Privacy Act (Cth) Part IIIA -- Credit Reporting
    Privacy Act (Cth) APP 7 -- Direct Marketing

Forms of Expression

- ... is exempt ...
- Despite ...
- {However} ... not ... if ...
- ... shall not ... unless ...
- ... other than ...
- ... not being ...
- ... do not apply to ...
- ... not in relation to / in respect of ...
- ... but does not include ...
- ... established ... otherwise than ...
- ... {an entity} other than ...
- ... is not covered by ...
- Except so far as the contrary intention appears, ...
- A permitted general situation exists in relation to ...
- ... a permitted purpose ...

- ... such steps as are reasonable in the circumstances …
- ... if it is practicable to specify ...
- ... in such form as is appropriate ...
- ... does not apply if ...
- ... unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities ...
- ... unless it is unreasonable or impracticable
- ... usually ...
- ... is likely to ...
- Despite ...
- ... reasonably believes ...

Sources

APF (2000-) '*Privacy Laws - Commonwealth of Australia*' and '*Privacy Laws - States and Territories*' Australian Privacy Foundation, 2000-

AustLII (2007-) '*Australian Privacy and Surveillance Law Library*' and 'International Privacy Law Library' AustLII and WorldLII, 2007-

Clarke R (1988) '*Information Technology and Dataveillance*' Commun ACM 31,5 (May 1988) 498-512

Clarke R (2014) '*The Regulation of Point of View Surveillance: A Review of Australian Law*' IEEE Technology & Society 33, 2 (Jun 2014) 40 – 46

Clarke R (2016) '*Privacy Impact Assessments as a Control Mechanism for Australian National Security Initiatives*' Computer Law & Security Review 32, 3 (May-June 2016) 403-418

Parker C (2007) '*Meta-Regulation: Legal Accountability for Corporate Social Responsibility?*' in McBarnet D, Voiculescu A & Campbell T (eds), *The New Corporate Accountability: Corporate Social Responsibility and the Law,* 2007

Waters N. (2006) '*Government Surveillance in Australia*' Pacific Privacy, August 2006

Williams G. (2011) '*A Decade Of Australian Anti-Terror Laws*' Melb. U. L. Rev. 35, 3 (2011) 1136-1176

Examples: [1] Mandatory DV

- ***Financial Transaction Reports Act (FTR Act) (Cth)***
  - Mandates cash dealers and solicitors to report to AUSTRAC transactions over A$10K, and to verify identities
- ***Anti-Money Laundering and Counter-Terrorism Financing Act (AMLCTF Act) (Cth)***
  - Financial institutions etc. must report suspicious and other transactions to AUSTRAC; must also comply with AMLCTF programs
- ***Telecommunications (Interception and Access) Amendment (Data Retention) Act (Cth) Schedule 1***
  - Mandatory metadata retention by ISPs, telcos etc.
  - Claims to 'put beyond doubt' that 'telecomm content' is not covered

Examples: [2 & 3] Permitted DV, & 'Permitted with conditions' DV

- ***Data-Matching Program (Assistance And Tax) Act (Cth)*** *s.6*
  - Authorises agencies to match data, subject to s.7 rules
- ***Privacy Act (Cth)*** *s.7B(4)*
  - "a media organisation is exempt ... if ... [it] is publicly committed to observe standards that ... deal with privacy ... and ... have been published"
    So the media achieved complete exemption,
    despite the absence of any controls over the contents of the 'standard'
- ***Surveillances Devices Acts*** (Victoria, WA and NT)
  - Prohibit use of visual and aural surveillance devices,
    but only if the person under surveillance has a strong case for expecting the behaviour would not be observed, transmitted or recorded

Examples: [4] Unregulated DV

- ***Privacy Act 1988 (Cth)*** s.6D:
  Personal data handling by small businesses < $A3m p.a
- ***Privacy Act 1988 (Cth)*** s.16:
  Personal data held for personal, family or household affairs
- ***Listening Devices Act 1991*** (Tas) s.5:
  CCTV (provided that no sound is recorded)
- ***The recording of images of children ?***
  (despite much moral breast-thumping from time to time)

Examples: [6 & 5] Prohibited DV, & 'Prohibited absent conditions' DV

- ***Telecomms (Interception and Access) Act (Cth) s.7***
  s.7(1) contains a general prohibition on interception
  But s.7(2) creates a dozen exceptions
- ***Queensland Criminal Code s.227A***
  Criminalises observation or visual recording made for the purpose of observing or visually recording another person's genital or anal region
- ***Australian Postal Corporation Act 1989 s.90N***
  The opening of an article, or the examination of its contents, is prohibited conduct ...
  But there are many exemptions in ss.90P-90UB

Practical Utility of a Model for Dataveillance Laws

1. **Assessment of laws against Privacy Meta-Principles**
   - May apply differently to different DV modalities
   - May enable consistent and comprehensive critiques of DV laws across modalities and technologies

Evaluation Meta-Principles to Reflect Multiple Stakeholder Interests

Pre-Conditions

1. Evaluation
2. Consultation
3. Transparency
4. Justification

Design

5. Proportionality
6. Mitigation
7. Controls

Post-Condition

8. Audit

Practical utility of a model for dataveillance laws

1. **Assessment of laws against privacy meta-principles**
   - May apply differently to different DV modalities
   - May enable consistent and comprehensive critiques of DV laws across modalities and technologies
2. **Recognition of novelty/severity in DV laws**
   - Useful to know if DV laws have no known precedents
   - Useful for comparisons with previous examples
   - Useful for developing measures of severity in options
3. **Assistance in comparing jurisdictions**
   - Comparing DV laws in different countries is difficult without categories independent of national experience
   - May provide a basis for indexing countries' intrusiveness

DV Law and 'Surveillance State'

- "A surveillance state is a country where the government engages in pervasive surveillance of large numbers of its citizens and visitors" (Wikipedia – too weak?)
- *Proposed definition of 'surveillance state:*
  A surveillance state is one in which
  pervasive surveillance is critical to the regime's survival
- *Relationship to DV Law:*
  A surveillance state places few prohibitions or conditions on state DV activities necessary to control political power
- DV Law Modalities 1-2, some 3-4, very few 5-6

DV Law and 'Surveillance Society'

- "Surveillance societies are societies which function, in part, because of the extensive collection, recording, storage, analysis and application of information on individuals and groups in those societies as they go about their lives" (Surveillance Studies Network – weak)
- *Proposed definition of 'surveillance society':*
  A society in which it considered normal for human activities to be subjected to DV, and many organisations utilise DV extensively
- *Relationship to DV Law:* A surveillance society places few prohibitions on non-state DV activities, and conditions involving data subject control are ineffective
- DV Law Modalities mostly 2-4, with few 5-6

... and 'Digital Surveillance Economy'

- **Digitisation** – The process of expressing data in machine-readable form (generally as a series of bits), or converting analogue data into digital form
- **Digitalisation** – The shift from the interpretation and management of the world through human perception and cognition, to processes that are almost entirely dependent on digital data
- **Digital Surveillance Economy** – That segment of the private sector in which revenue and profit derive from the expropriation and exploitation of personal data
- **Surveillance Capitalism** – "information capitalism that predicts and modifies human behavior as a means to produce revenue and market control" (Zuboff 2015)

Dataveillance Law:

Modalities, Categories and Examples

Roger Clarke and Graham Greenleaf

Xamax, UNSW Law, ANU RSCS, APF and UNSW Law, APF, AustLII

5th Asian Privacy Scholars Network Conference, Auckland, Dec. 2016

Roger.Clarke@xamax.com.au and graham@austlii.edu.au