Towards best practice Privacy Principles

Nigel Waters and Graham Greenleaf
Cyberspace Law & Policy Centre, UNSW

Meeting Privacy Challenges – The ALRC and NSWLRC Privacy Reviews

Sydney, 2 October 2008

Key points

- Coverage of Federal privacy law
  - Better coverage, but danger of levelling down
- Structural approach to privacy regulation
  - Sensible aspirations, but many dependencies
- Principles
  - Some improvements, some losses, many missed opportunities
- Prescription vs Guidance
  - Trust in guidance misplaced in light of experience
- Sectoral regulation
  - Open invitation for special pleading and weaker protection

Proposed Principles

- **Proposals which give individuals *more* control or otherwise limit surveillance**
  - **but in most cases with serious limitations.**
- **Proposals which give individuals *less* control or otherwise increase surveillance**
- **Missed opportunities to strengthen control or otherwise limit surveillance**
- **Proposals relating to other objectives**
  - **downstream safeguards – mostly positive**

INTERPRETING PRIVACY PRINCIPLES

More control

- application of most UPPs to agencies (* but some losses)
- inclusion of biometric information in the definition of 'sensitive information' (Rec 6-4) (* but constrained)
- addition of 'pseudonymous' to the 'Anonymity' principle (UPP1) and application to agencies (*but cannot be effective unless proactively enforced)
- removal of the 'mere awareness' exception to the disclosure principle currently applying to Commonwealth agencies (UPP 5)
- strengthening of the Direct marketing principle (UPP6) but not applied to agencies
- extension of the Identifiers principle (UPP10) (* but not to Commonwealth agencies)
- application of the Cross-border data flow principle (UPP 11) to agencies (* but weak in effect)

Less control

- ALRC view that data linkage arrangements where identification keys are held by third parties amounts to de-identification (6.72, 6.83)
- removal of 'imminent' from the 'harm' exceptions UPP 2.5(c); UPP 5.1(c) and UPP 9.1(b)
- increasing the freedom with which organisations are able to transfer personal information overseas, including to countries with weak or non-existent privacy laws (UPP 11)

Missed opportunities

- core definitions such as ‘personal information’ remain unchanged
- 'publicly available information' unresolved
- obtaining by observation, by extraction from other records, and by internal generation (from transactions) still not expressly 'collection'
- no additional conditions on the collection of 'sensitive' personal information
- failure to add 'specifically' to the 'authorised by or under law' exceptions
- failure to recommend key elements of 'consent'
- no binding rules for automated decision-making or data-matching
- security obligation not expressly applied to collection
- primary purpose(s) not clearly linked to the purpose *of collection*

Other positive proposals

- Handling of unsolicited information (UPP 2.4)
- Notification requirements for both direct and indirect collection (UPP 3)
- Data quality principle (UPP 7) strengthened
- Access and correction principle (UPP 9) generally strengthened (* but FOI review in limbo?)
- Third-party intermediary access (UPP 9.3)
- Notification of corrections to recipients (UPP 9.6(b)) *
- Requirement to disclose overseas transfer practices, and likely destinations, in privacy policies (UPP 4.1(c)) *
- Requirement for disclosure of data breaches (Rec 51-1) (* but weak)
- Requirement to make privacy policies available electronically (UPP 4.2(a)) *

INTERPRETING PRIVACY PRINCIPLES