Privacy Principles for Identity Management[1]

Professor Charles Raab
University of Edinburgh

Keynote Presentation at the PrimeLife/IFIP Summer School
Nice, 7-11 September 2009

[1] based on and expanded from Scottish Government: *Privacy and Public Confidence in Scottish Public Services: Draft Identity Management and Privacy Principles*, Consultation Document, 31 August 2009.

Why Necessary?

To tailor general privacy principles to specific identity system applications, as with codes of practice

For public services organisations' policy-makers and practitioners involved with identity or entitlement systems (and more generally as well)

To help overcome tunnel vision on 'security'

EU Directive 95/46/EC (Recital 46): 'technical *and organizational*' security measures (emphasis added)

Danger of 'technicalising' better data handling under current post-breach initiatives

Need to build into pan-organisational processes and 'culture'

People are justifiably concerned, or ought to be, about lack of transparency, redress, and excessive data *collection*, *sharing*, and *storage*

All of these are addressed by good data-protection practice, and should not be seen

Principles regarding...

‘Proving’ identity and/or entitlement

Accountability and organisational governance

Dealing with risk

Data processing and sharing: privacy risk reduction

Public engagement and education

‘Proving’ identity and/or entitlement

Identification only if necessary, not routinely

Minimise information asked for

Allow choice of ways if possible

Ensure reliability of identification mechanisms, and convenience

Avoid exclusion and discrimination

Identify only once if possible, verify *entitlement* thereafter

Reciprocate: identify your organisation

Accountability and organisational governance

- Ensure compliance with letter and spirit of law and data protection principles
  - consider privacy as a *right*, not a (consumer) *preference*
  - duty of care to members of the public
  - consent where necessary
- Adopt robust organisational policies and procedures for privacy (including security) in identity management; e.g.:
  - encryption, etc.
  - access logs and internal audit
  - metadata
  - procedures for reporting and external oversight
- Clearly designate responsibility at high level and below
- Take staff training seriously and undertake it continuously

Dealing with risk

Privacy impact assessment (PIA) for new initiatives

- conducted early
- not 'box-ticking'/ 'prayer wheel'
- made publicly available
- report to parliamentary committee considering legislation

Audit for old systems

Develop an approach to understanding and dealing with risk

- 'risk' is to *privacy* or other citizen values, not (necessarily) to the organisation or its reputation
- understand what the public finds risky
- also consider what the public *ought to* find risky
- how much precautionary *anticipation* of worst cases ('just-in-case')?
- how much *resilient* coping ('firefighting')?

Data processing and sharing: privacy risk reduction

Minimise collection, sharing, and storage

necessity and *proportionality*

Avoid single centralised databases if possible

Separate basic personal and transactional data if possible

need to store identifying information?

Strict access control

Avoid sharing identifiers if possible

Public engagement and education

Raise public awareness of identity processes and risks

Help people to make more informed decisions

Provide access and redress

Learn from the public about their apprehensions

Take engagement and education seriously and avoid:

- just going through the motions
- doing it too late
- patronising the public

Questions for discussion...

What is missing?

Can these principles be implemented, or are they just a wish list?

What are the obstacles?

What resources, including leadership, would be needed?

What would be the consequences of failure?

In terms of trust and implementability, is there a difference between 'identity management' (reflecting the interests of database owners) and 'identity assurance' (individual-led)?

Consultation responses to…

http://www.scotland.gov.uk/privacyprinciples2009

before: 23 November 2009

Document available at:

http://www.scotland.gov.uk/Publications/2009/08/PrinciplesConsultation