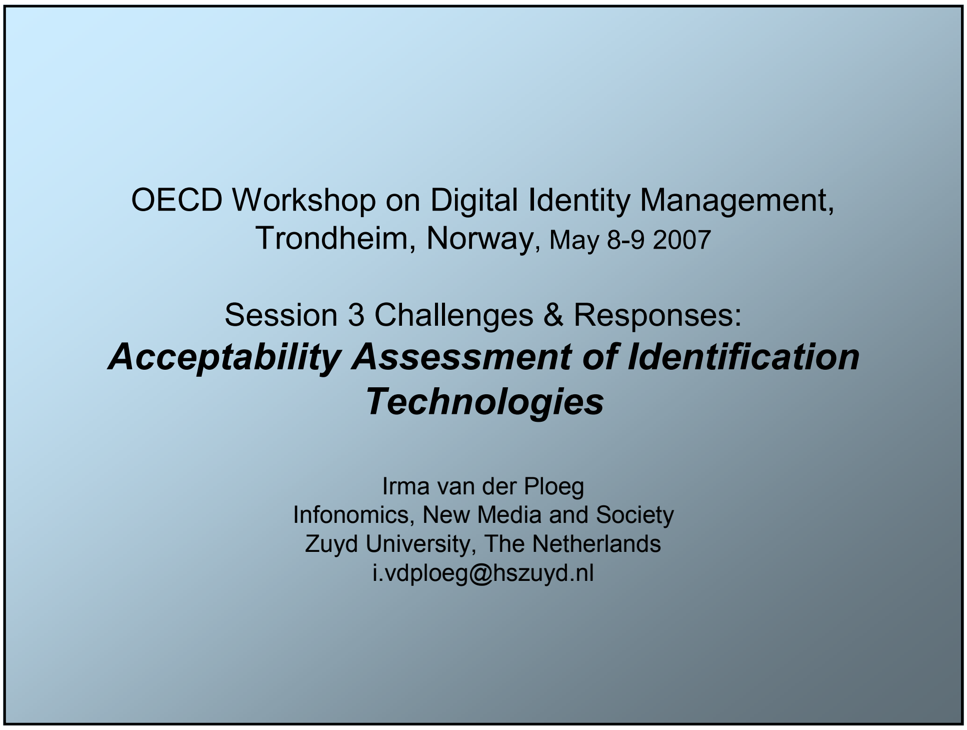
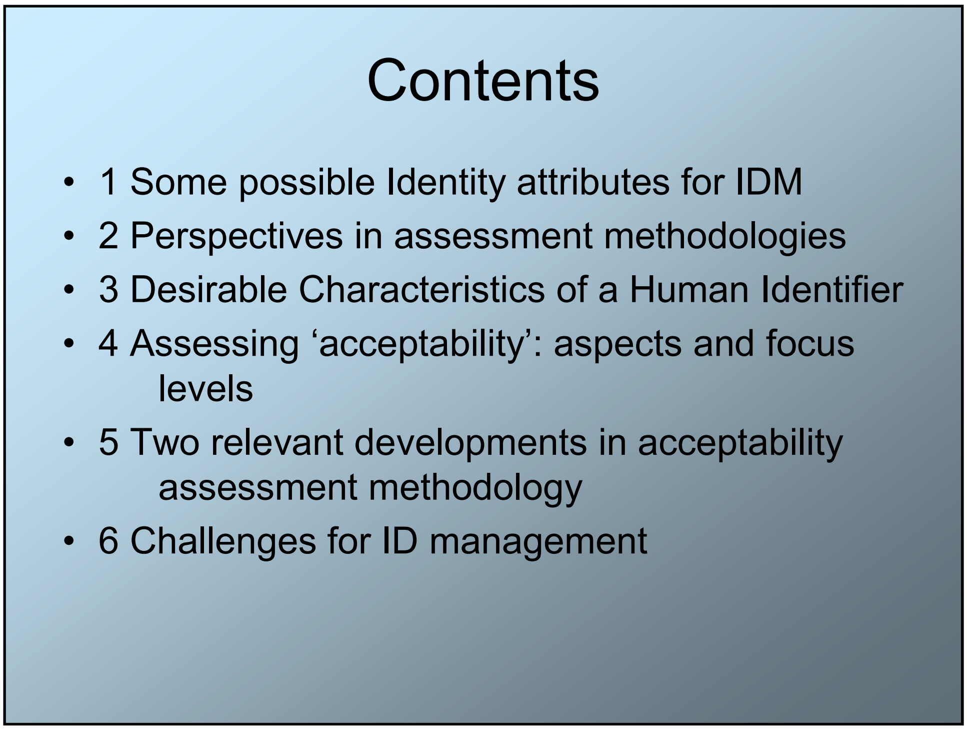


OECD Workshop on Digital Identity Management,
Trondheim, Norway, May 8-9 2007

Session 3 Challenges & Responses:

Acceptability Assessment of Identification Technologies

Irma van der Ploeg
Infonomics, New Media and Society
Zuyd University, The Netherlands
i.vdploeg@hszuyd.nl



Contents

- 1 Some possible Identity attributes for IDM
- 2 Perspectives in assessment methodologies
- 3 Desirable Characteristics of a Human Identifier
- 4 Assessing ‘acceptability’: aspects and focus levels
- 5 Two relevant developments in acceptability assessment methodology
- 6 Challenges for ID management

1 Some possible Identity attributes for IDM

- social behaviour - or how the person interacts with others;
- names - or what the person is called by other people;
- codes - or what the person is called by an organisation;
- knowledge - or what the person knows;
- tokens - or what the person has;
- Date of birth
- National registration number (SSN, BSN)
- Biometric

2 Perspectives in assessment methodologies

- Cost-benefit ratio
- Organisational needs
- Public needs
- Other challenges: legal, ethical, socio-political, and human rights issues

3 Desirable Characteristics of a Human Identifier

- **universality of coverage** : every relevant person should have an identifier
- **uniqueness** : each relevant person should have only one identifier , no two people should have the same identifier
- **permanence** the identifier should not change, nor be changeable
- **collectibility** : the identifier should be collectible by anyone on any occasion
- **storability** : the identifier should be storable in manual and in automated systems
- **precision** : every identifier should be sufficiently different from every other identifier that mistakes are unlikely
- **simplicity** : recording and transmission should be easy and not error-prone
- **cost** : measuring and storing the identifier should not be unduly costly
- ***convenience*** : measuring and storing the identifier should not be unduly inconvenient or time-consuming
- ***acceptability*** : its use should conform to contemporary social standards

Cf Roger Clarke, 1994

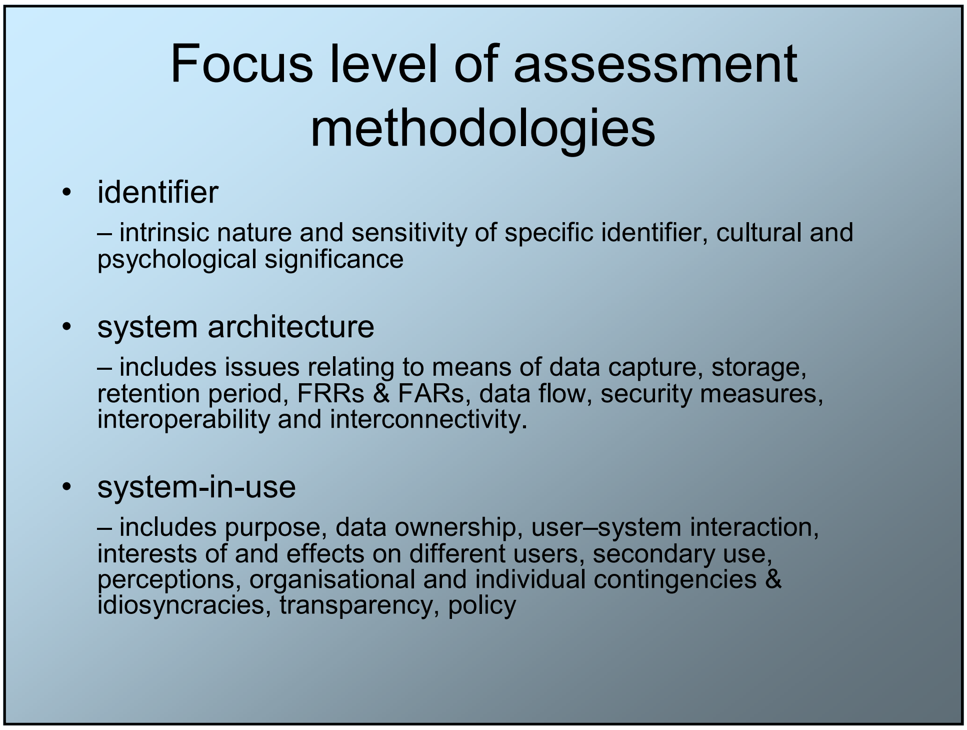
4 ‘Acceptability’ ?

Clarke:

‘its use should conform to contemporary social standards’

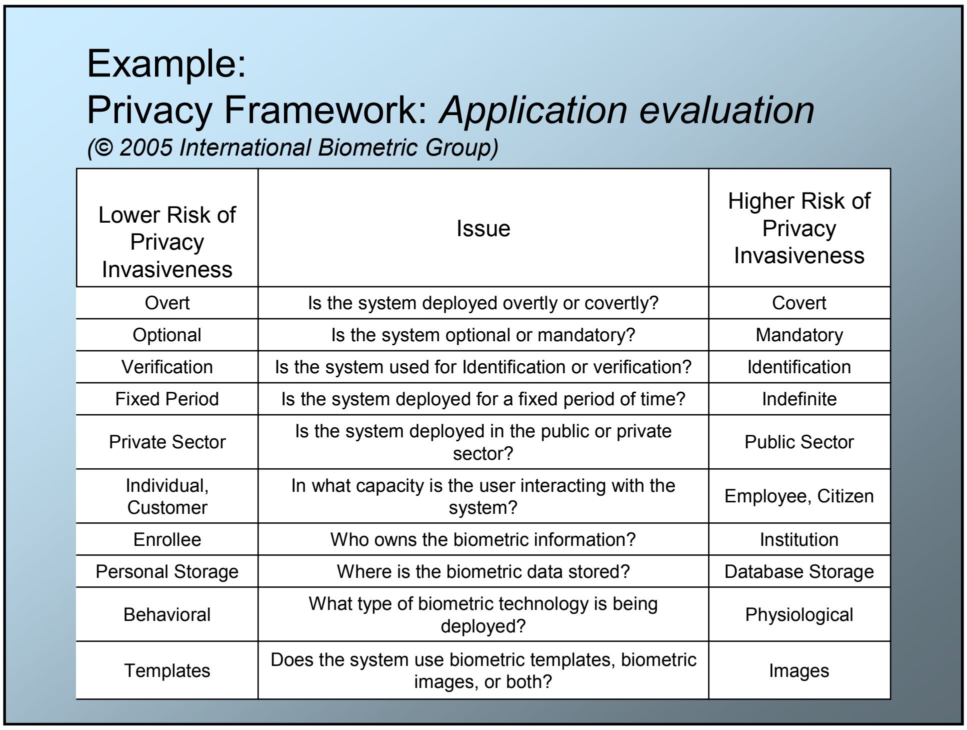
- Whose standards, concerning what exactly?
- To what extent may consensus be assumed?
- Should include: Legal, ethical, socio-political, human rights norms & standards

- How to assess ‘acceptability’ in this wider sense?



Focus level of assessment methodologies

- identifier
  - intrinsic nature and sensitivity of specific identifier, cultural and psychological significance
- system architecture
  - includes issues relating to means of data capture, storage, retention period, FRRs & FARs, data flow, security measures, interoperability and interconnectivity.
- system-in-use
  - includes purpose, data ownership, user–system interaction, interests of and effects on different users, secondary use, perceptions, organisational and individual contingencies & idiosyncracies, transparency, policy



Example:
Privacy Framework: *Application evaluation*

(© 2005 International Biometric Group)

Lower Risk of Privacy Invasiveness	Issue	Higher Risk of Privacy Invasiveness
Overt	Is the system deployed overtly or covertly?	Covert
Optional	Is the system optional or mandatory?	Mandatory
Verification	Is the system used for Identification or verification?	Identification
Fixed Period	Is the system deployed for a fixed period of time?	Indefinite
Private Sector	Is the system deployed in the public or private sector?	Public Sector
Individual, Customer	In what capacity is the user interacting with the system?	Employee, Citizen
Enrollee	Who owns the biometric information?	Institution
Personal Storage	Where is the biometric data stored?	Database Storage
Behavioral	What type of biometric technology is being deployed?	Physiological
Templates	Does the system use biometric templates, biometric images, or both?	Images

5 Two relevant developments in approaching social and ethical acceptability assessment:

- Ethics of technology and engineering:

From individual responsibility to collective co-responsibility

(C. Mitchum, R. von Schomberg, and others)

- Interdisciplinary Science & Technology Studies:

From social and ethical impact assessment to analysis of normativity in technological practices

(L. Winner, B. Latour, M. Akrich, and others)

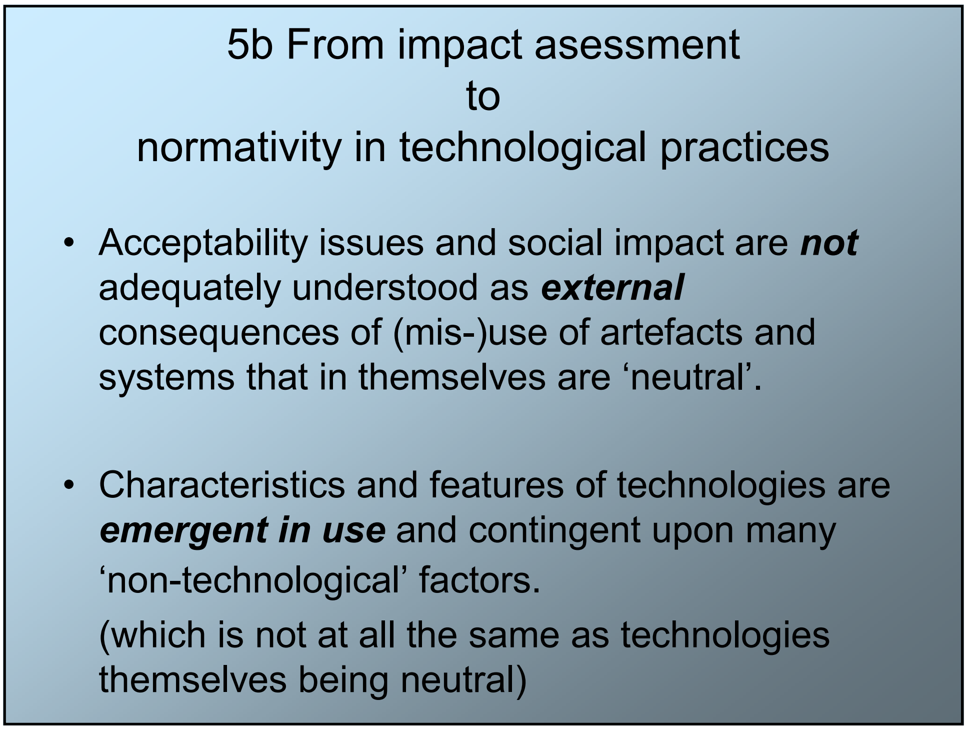
5a From individual responsibility to collective co-responsibility

The problem with individual ethical responsibility

- Specialization, proliferation, compartmentalisation of roles, expertise, knowledge, and institutional arrangements, make individuals less and less able to oversee, predict, or control consequences of their actions and designs.

Collective co-responsibility demands for collective decisionmaking informed by :

- Strategic foresight knowledge
- Collective interdisciplinary deliberation at the interface of spheres
- Transparent technology assessments
- Public debate

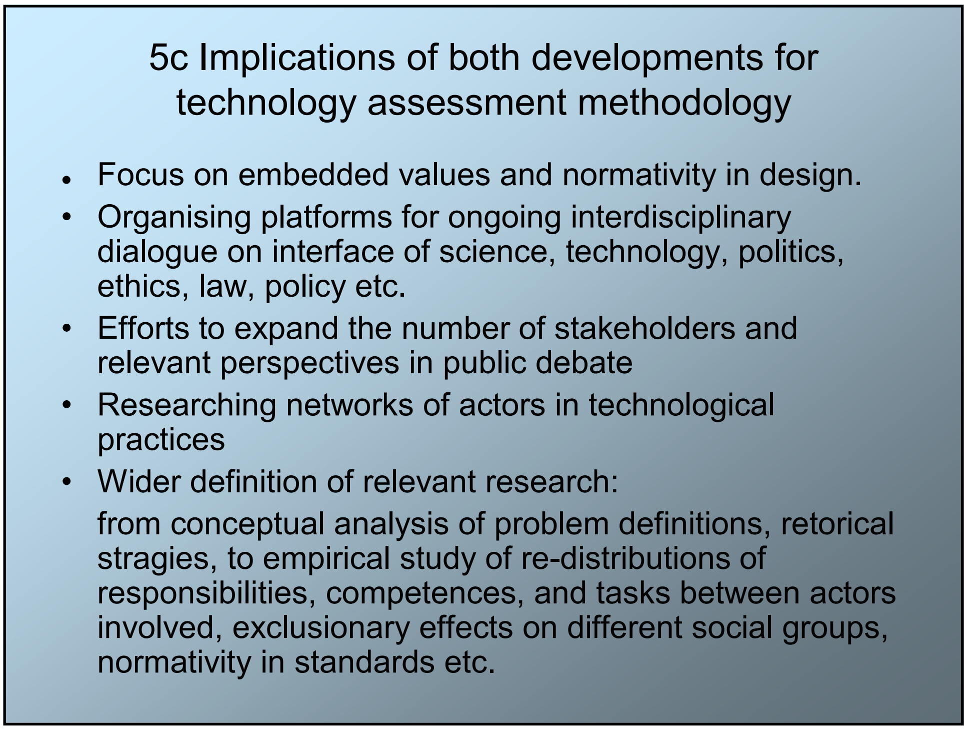


5b From impact asessment to normativity in technological practices

- Acceptability issues and social impact are ***not*** adequately understood as ***external*** consequences of (mis-)use of artefacts and systems that in themselves are ‘neutral’.

- Characteristics and features of technologies are ***emergent in use*** and contingent upon many ‘non-technological’ factors.

  (which is not at all the same as technologies themselves being neutral)



5c Implications of both developments for technology assessment methodology

- Focus on embedded values and normativity in design.
- Organising platforms for ongoing interdisciplinary dialogue on interface of science, technology, politics, ethics, law, policy etc.
- Efforts to expand the number of stakeholders and relevant perspectives in public debate
- Researching networks of actors in technological practices
- Wider definition of relevant research:

  from conceptual analysis of problem definitions, retorical stragies, to empirical study of re-distributions of responsibilities, competences, and tasks between actors involved, exclusionary effects on different social groups, normativity in standards etc.

6a Challenges for ID management

- Digital identification procedures *create* security and privacy risks (skimming, phishing, hackable databases etc.) – limit ID to where it is strictly required; maximise PETs, pseudonymity, anonymity
- Universal identifiers (e.g. biometrics) exacerbate security and privacy risks; design for *context/domain specific* digital identities.
- Different definitions and forms of ‘*security*’ lead to contradictory priorities in IDM system design.

6b Challenges for ID management

- Managing digital identity not to remain prerogative of system owners but to be defined as right of end-user; design for more *end-user control*
- Analyse ‘technical issues’ (successrates, standards and interoperability issues etc.) as normative/political issues
- Assess IDM in relation to wider technological/legal/policy configuration, e.g. interdisciplinary analysis of specific application areas.
- *Transparency*- lack thereof on all levels

  (system design, policy & decisionmaking, legal context, actors involved, secondary use of personal data)

  precludes significant public debate, informed citizens/customers, exercise of control or rights. – transparency - interdisciplinary debate and research are called for urgently

Thank you
for your attention.

* * *