Mission creep:
biometrics and security

Prof. Juliet Lodge & Daniel Nagel

Jean Monnet European Centre of Excellence
University of Leeds UK

Brussels 30 January 2010

Function creep to mission creep

- the story of biometrics in the EU
  - how law is left behind
  - examples of mission creep
  - legal remedies (the German experience and response)
  - insufficiency of what exists now to deal with life today and certainly completely inadequate for life tomorrow in AmI
  - ethical questions
  - future suggestions

EU versus US --- the risk of new biometrics

- Biometrics nothing new
- What is new is that the EU has in practice accepted (at least in some states, UK, NL) the US definition of a biometric
- In 2001 – it was no more than an algorithm; in 2009 it was a behaviour based ‘profile’
- Profiling can be subjective, is designed to be discriminatory
- So what’s the problem?

Problems

Legal

- Conflict with laws on human rights, fundamental freedoms and quintessential equality of EU citizens
- Proportionality of the use of biometrics

Social --- a shift to arbitrariness

- Creation of social division/social sorting/exclusion/ impact on infirm and young

Inclusion and Exclusion

- Belonging and citizenship for inclusion

  US the 'good' in-group

  THEM the untrusted out-group

- Use of state rules and rights to include and exclude (eg for security)

- profiling; biometrics; borders; migration

  Is there an emerging lexicon of proportionality?

Slippery slope to justify *dis*proportionality & Mission creep

- *Biometric-border controls* – epassports for entry exit tracking certainty
- **Failures** – Spoofing : Biometric by itself insufficient
- '**Solution**' --- widen definition to include 'intelligence criteria' (thereby intruding on privacy and human rights and dignity)

Panopticon = dangers of mission creep

Dangerous and unethical?
Law lags behind ambient intelligence

- Data subject does not know he is tracked
- Banking and e-commerce outsourced to states/companies who re-outsource to others to evade data protection rules
- Data information industry growth means data subject ceases to ‘own’ it in any real sense
- Data protection is high on rhetoric and LATE on impact

What we have instead of sufficient law is …..

- Emerging lexicon of proportionality around ideas of an ICT test of *fitness-for-purpose*

  E.g. it can be designed to limited reach of automated information exchange for border control and policing purposes (Stockholm Prog)

  Mission creep inevitable when the number of agencies allowed to access a data base expands - as it is doing

Necessary measures v. important public interests

- Contingent - No absolute answer
- Revision of legislation always possible

  E.g. US Patriot Act (2001) amendment of Foreign Surveillance Act (FISA) to allow government to do broad based surveillance in US for 'SIGNIFICANT PURPOSE' to obtain foreign intelligence less stringent that the previous 'PRIMARY PURPOSE' requirement.

  District Court struck it down because it failed to meet the 'probable cause' requirement

- Proportionality, purpose limitation, data minimisation principles
- Is proportionality a lost cause?

ICTs as solution to PROBLEM OF DIVERSE SYSTEMS

Multiplicity of

- languages (21 +)
- legal systems (30+)
- administrative authorities : police, frontier guards, immigration officers (60+) –
- Should there be one central border guard? Whose legal system should control it? Operational remit? Who funds it? Do biometrics outsource or relocate responsibilities to 'richer' states or companies?

Secure borders : Underlying premise

- Primacy of security over privacy
- Sustaining F S J requires respect for the rule of law
- Border security requires effective judicial, customs, border, immigration and police cooperation
- IT can boost border management cooperation
- Ecooperation using biometrics can enhance crime detection, protect borders, crime busting in EU and outside EU and so help to sustain FSJ
- Security is more important than privacy

Primacy of security and risk-free

Prioritising risk-free world means that ultimately anything that could ‘pose a threat’ is a potential ‘security risk’

Danger that the RULE OF LAW is being rapidly eroded by commercial interests selling ‘security’

(dis) proportionate biometrics?

- Multiple ID documents
- RFID implants (RSPCA; bars; goods – ambient)
- Enrolment at visa posts/outsourced
- Soft biometrics
- DNA use as a biometric versus sampling and profiling AND need for centralised data bases

Proportionality is always contingent

Contingency reflects perceptions of risk to privacy and security

Complacent ducking of responsibility for incredible claims

- Info power and abuse of power
- Reduce discretionary non-disclosure and exceptions ----- vigilance of NPs and EP
- Query necessity of mission creep that adds to exceptions (e.g. security and financial exemptions)
- Legal compliance failures
- Dangerous out-sourcing and re-outsourcing to PPPs

What society do we want?

Problems of Trust and Credibility of Data Protection

and respect for the law

Who is trusted? Is there a trusted regulator?

- Are the European Parliament and national parliaments irrelevant?
- Ombudsmen
- Data protection supervisors
- Technology developers
- Public low confidence in data protection and government

Vigilance for the common good

- Proportionality in privacy and trust?
- What role should parliaments play in safeguarding citizens?
- Is it too late to define and enforce a

  ethical code in an arbitrarily sorted society reliant on mini robots in ambient intelligent environments?

Communicating ICTs and security

‘Citizens must be able to understand the system so that they can identify its problems, criticise it, and ultimately control it.’

Final report of the Convention on the Future of Europe

Working Group IX on Simplification 29 Nov 2002

[CONV 424/02 WGIX 13]

Juliet Lodge j.e.lodge@leeds.ac.uk

Thank you for listening

Contacts

Juliet Lodge j.e.lodge@leeds.ac.uk

Daniel Nagel icsbest@leeds.ac.uk