

# Privacy Impact Assessments The UK experience

Dr Adam Warren  
Loughborough University



# The Project

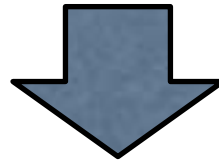
- Commissioned by UK ICO
- July – December 2007
- 5 project partners
- Remit:
  - International study
  - Handbook

# What are PIAs?

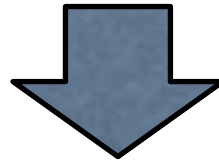
- ‘A systematic risk assessment tool that can be usefully integrated into decision-making processes’
- Examples: Canada, Australia, New Zealand and United States
- Various tools: handbooks, eLearning tools
- Notable handbooks:
  - Australian Privacy Commissioner (2006)
  - New Zealand Privacy Commissioner (2002)
- Another option:
  - eLearning Tool (Canada, 2003)  
[http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-a\\_e.asp](http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index-a_e.asp)
- June 2008: mandatory in UK central govt departments

# PIA Screening Tool

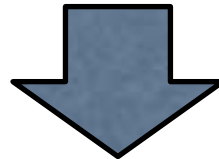
STEP 1 – Is a Full-Scale PIA necessary?



STEP 2 – Is a Small-Scale PIA necessary?



STEP 3 – Is Privacy Law Compliance Checking necessary?



STEP 4 – Is Data Protection Act Compliance Checking necessary?

# User Interest

- Aegate: privacy implications of using RFID technologies to authenticate prescription pharmaceuticals at point of sale\*
- Department for Transport: privacy implications of national time - distance-place road pricing policy\*
- NPIA: Police National Database ...
- Attracted interest overseas
  - Netherlands DP Authority
  - Swedish Data Inspection Board
  - European Data Protection Supervisor

\* Conducted by Enterprise Privacy Group

# Lessons Learnt

- Internal stakeholder resistance to process\*
- External stakeholder reluctance to engage\*
- Lack of accountability
- Need to be prospective – identify privacy risk *before* systems put in place
- Need to refer to entire process of assessment of privacy risk, more than the end-product or statement
- Need to have potential to alter proposed initiatives; should not be mechanical ‘tick box’ exercise

\*Refer: <http://www.esrc.ac.uk/ESRCInfoCentre/about/CI/events/esrcseminar/privacyimpact.aspx>

# Future Development

- To what extent can technologies aid PIAs? [EPSRC project]
- What is the role for PIAs in assessing compliance and risk for new types of infrastructure i.e. cloud computing?
- How might automated risk assessment be provided / improved?
- Can different strategies be used for performing PIAs in key commercial sectors?