The state of the art in privacy impact assessment

David Wright
Managing Partner
Trilateral Research & Consulting
at the IAPP Congress
Brussels
14 November 2012
Outline

• Privacy breaches & intrusions
• Origins of PIA
• Current status – Article 33
• A step-by-step guide to PIA
• Benefits of PIA (it’s not all scary)
• Further reading
Privacy breaches & intrusions

• “British Airways flies into privacy storm over Google identity checks on passengers”, *London Evening Standard*, 5 July 2012
• “Global Payments cops to 1.5 million total on credit card breach”, *Infosecurity*, 2 April 2012
• “ICO fines Midlothian Council £140,000- ICO's highest ever fine for data breaches”, *Lexology*, 1 March 2012
• “Facebook security breach raises concerns”, *The Washington Post*, 16 November 2011
More privacy breaches & intrusions

- “Google Snoop View: Search engine giant 'knew its software could steal emails, pictures and text messages from millions of people with its Street View cars’”, *Daily Mail*, 27 May 2012
- “Smart meters are 'massive surveillance' tech - privacy supremo”, *The Register*, 11 June 2012
- “EU hands personal data to US authorities on daily basis”, *EU Observer*, 22 June 2012
Definition of PIA

- A process for assessing the impacts on privacy of a project, technology, service, policy or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts.

- A PIA is about identifying risks and finding solutions, not simply producing a report that demonstrates compliance.
Origins of PIA

- Environmental impact assessments
- Technology impact assessments
- Australia
- Canada
- New Zealand
- US
- Deloitte & Touche – Guide to Cross-Border PIAs, 2001
- ISO PIA voluntary standard for financial services, 2008
PIA in Europe

• UK Information Commissioner’s Office (ICO), PIA Handbook, 2007 (rev. 2009)
• Slovenian Information Commissioner's Guidelines: PIA in e-Government Projects, July 2010
• Irish Health Information and Quality Authority, PIA Guidance, Dec 2010

• EC RFID Recommendation in May 2009
• Art. 29 WP “endorses” RFID PIA framework, Feb 2011
• PIAF project, Jan 2011 – Oct 2012
Current status of PIA in EU

• CEN TC 225 is examining prospects for standardisation for RFID PIA
• Several countries (Netherlands, Denmark, Finland) have been considering PIA policies or handbooks
• Art. 33 of the EC’s proposed Data Protection Regulation, released 25 Jan 2012
• ISO beginning work on a standard for PIA by 2015
Article 33

• Obliges data controllers to carry out a “data protection impact assessment” where processing presents “specific risks to the rights and freedoms of data subjects”

Art. 33(2) cites examples of such risks:
• a systematic and extensive evaluation of a person's economic situation, location, health, personal preferences, reliability or behaviour
• information on sex life, health, race and ethnic origin
• video surveillance
• genetic or biometric data
• other processing operations requiring consultation with the DPA
Article 33 (cont’d)

Art. 33 (3) describes what the assessment shall contain:
• a description of the envisaged processing operations,
• an assessment of the risks
• measures to address the risks
• safeguards to ensure protection of personal data
• compliance with this Regulation

• Art. 33 (4) -- The controller shall seek the views of data subjects

• Art. 33 would empower the EC to adopt “delegated acts” re verifying and auditing the assessment
PIAF project

• Funded by DG Justice
• Consortium of VUB, Trilateral & PI
• Reviewed PIA policies and practices in Australia, Victoria state, Canada, Ontario, Alberta, Hong Kong, Ireland, New Zealand, UK and US
• Surveyed EU DPAs re their views on PIA
• Recommended an optimised PIA based on best practices
• Three workshops for EC policy-makers & Art. 29 members
State of the art in PIA

- “Step-by-step guide to privacy impact assessment”
- “A template for a PIA report”
A step-by-step guide to PIA (1)

1. Determine whether a PIA is necessary (threshold analysis)
2. Identify the PIA team and set the team’s terms of reference, resources and time frame
3. Prepare a PIA plan
4. Determine the budget for the PIA
5. Describe the proposed project to be assessed
6. Identify stakeholders
7. Analyse the information flows and other privacy impacts
8. Consult with stakeholders
A step-by-step guide to PIA (2)

9. Check the project complies with legislation
10. Identify risks and possible solutions
11. Formulate recommendations
12. Prepare and publish the report, e.g., on the organisation’s website
13. Implement the recommendations
14. Third-party review and/or audit of the PIA
15. Update the PIA if there are changes in the project
16. Embed privacy awareness throughout the organisation and ensure accountability
Template for a PIA report (1)

1. Cover page
2. Executive summary
3. Introduction and overview of the PIA process
4. Threshold assessment
5. Project description
6. Information flows
7. Privacy impacts (risks)
8. Organisational issues
9. Options and alternatives
10. Design features to avoid privacy intrusion
11. Compliance with laws, regulations, codes and guidelines
12. Stakeholder analysis
13. Results of the consultation(s)
14. Recommendations
Contentious issues = state of the art

• Mandatory PIA
• A PIA is more than a compliance check
• Stakeholder engagement
• Publication of the PIA report
• Third party review or audit (have the recommendations been implemented?)
• PIA is a process (the report is not *the* objective)
• All types of privacy, not just data protection
• Trans-national PIAs
• PIA of policy & legislation
• A central registry of PIAs
• Should a DPA approve a PIA?
Benefits of PIA

- An early warning system, a way to detect privacy problems, build safeguards before, not after, heavy investment – Fix privacy problems now, not later
- Avoids costly or embarrassing privacy mistakes
- Provides evidence that an organisation attempted to prevent privacy risks (reduce liability, negative publicity, damage to reputation)
- Enhances informed decision-making
- A way to gain the public’s trust and confidence
- Demonstrates to employees, contractors, customers, citizens that the organisation takes privacy seriously
Further reading

PIA projects

• PIAF – Privacy Impact Assessment Framework
  www.piafproject.eu

• PRESCIENT – developing a combined privacy and ethical impact assessment framework
  www.prescient-project.eu

• SAPIENT – developing a surveillance impact assessment methodology
  www.sapientproject.eu

• www.trilateralresearch.com