Should privacy impact assessments be mandatory?

David Wright
Trilateral Research & Consulting
17 Sept 2009

Today's presentation

- Databases – solving one problem & creating another
- What is a privacy impact assessment?
- Variations in PIAs – UK & Canada
- Benefits & disadvantages
- The case for & against mandatory PIAs
- Beyond mandatory PIAs – audits & metrics
- Conclusions

ContactPoint

- Abuse & death of eight-year-old child in 2000 led to inquiry & report in 2003 by Lord Laming
- Victoria's death could have been prevented if there had been better communication between social services
- Led to creation of a database, called ContactPoint
- Government said the database would improve child protection by improving way information about children is shared
- ContactPoint launched in Jan 2009 holds data on 11 m children

ContactPoint (cont'd)

- Database was designed to solve one set of problems but created another set of problems
- It has attracted significant criticism over the risks to privacy and personal data protection
- Some 330,000 people have access to the database
- Richard Thomas: "Is collection of personal information about every child a proportionate way to balance opportunities to prevent harm and risks of misuse?"
- "A PIA would enable better decision-making & demonstrate how questions of proportionality are being addressed"

Citizens' views

- Eurobarometer report on citizens' perceptions of data protection in the EU in 2008:
- 64 per cent said they were concerned about the protection of privacy
- A slight increase over similar poll in 2003
- Little change since first poll in 1991 when two-thirds said they were concerned
- Public is right to be concerned as shown by numerous breaches of databases & losses of personal data in government & industry
- PIAs are a tool for addressing the risks

What is a privacy impact assessment?

- A systematic process for evaluating the potential effects on privacy of a project, system or scheme and ways to mitigate or avoid any adverse effects
- Term first used in a Canadian Justice Committee document in 1984
- 2 PIA drivers:
- Public reaction to privacy-invasive actions of governments & corporations
- Organisations' recognition of privacy as a strategic variable & need to factor it into risk management.

PIA should take into account four aspects of privacy

- Privacy of personal information – others have our data
- Privacy of the person – body searches, biometric measurement
- Privacy of personal behaviour – surveillance, media intrusion
- Privacy of personal communications – telephonic intercepts, monitoring e-mail, etc.

What PIAs are not

- Compliance checks
- Audits

- Prior checking – Data Protection Directive Art 20: “Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.”

Who is using PIAs?

- Australia
- Canada
- Hong Kong
- New Zealand
- UK
- United States
- ISO – has produced a standard for PIAs in financial services
- Some companies – e.g., Vodafone, Phorm

The UK PIA process - 1

- In Dec 2007, the UK ICO published its PIA manual (with a 2nd version in June 2009)
- PIA process should begin asap, when the PIA can affect development of the “project”
- Aims to identify privacy impacts
- Understand & benefit from views of stakeholders
- Understand acceptability of projects & how people might be affected
- Identify less privacy-invasive alternatives
- Avoid or mitigate negative impacts on privacy
- Document & publish the outcomes of the PA process

The UK PIA process - 2

- PIA manual has screening questions to determine if a PIA is necessary and, if so, whether a full-scale or small-scale PIA
- Scope of the PIA depends on size of the organisation, sensitivity of data, the risks, the intrusiveness of the technology, etc
- Full-scale PIA has five phases:
  - Preliminary
  - preparation
  - consultation & analysis
  - documentation
  - review & audit

The UK PIA process - 3

- Preliminary phase – establish terms of reference, scope & resources
- Prepare a background paper for discussion with stakeholders, which describes…
  - the project's objectives,
  - scope,
  - business rationale,
  - the project's design,
  - initial assessment of potential privacy issues & risks,
  - options for dealing with them,
  - list of stakeholders to be invited to contribute

The UK PIA process - 4

- Preparation phase:
- Stakeholder analysis, consultation plan
- Establish a PIA consultative group (PCG), comprising representatives of stakeholders
- Distribute background paper to PCG

- Consultation and analysis phase:
- Consultation with stakeholders
- Risk analysis – identifying problems & solutions
- Deliverables – issues register, privacy design features paper, possible changes to the project design

The UK PIA process - 5

- Documentation phase – documents the PIA process & outcomes in a report to be made public.

Reasons for a PIA report:

- Accountability
- Provides basis for post-implementation review & audit
- Provides corporate memory & enables sharing of experience

The UK PIA process - 6

- The PIA report should contain:
- A description of the project
- Business case justifying privacy intrusion & its implications
- Discussion of alternatives & rationale for decisions taken
- A description of the design features adopted to reduce / avoid privacy intrusions
- An analysis of the public acceptability of the scheme

- Review and audit phase

The Canadian PIA process - 1

- Mandatory PIA policy adopted in May 2002
- Requires that PIAs be conducted on all new government initiatives that raise privacy risks
- PIA results to be shared with the Office of the Privacy Commissioner (OPC)
- PIA summaries to be posted on websites
- PIA policy responsibility lies with Treasury Board Secretariat (TBS)

The Canadian PIA process - 2

- Protection of privacy is one of the most important issues facing Canada in the next 10 years
- Onus is on institutions to demonstrate that their collection and use of personal information respects the Privacy Act of 1983 and the PIPEDA Act of 2000
- Obliges institutions to communicate with citizens why their personal data is being collected, how it will be used and disclosed, and how privacy impacts will be resolved

The Canadian PIA process - 3

- TBS has produced a PIA handbook
- Like ICO, the OPC views PIA as a process
- PIA guidelines are intended to anticipate, prevent, mitigate negative consequences to privacy
- PIA to be initiated at early stage of designing a program or service
- PIA is an iterative process that continues throughout the life cycle of the program or service

The Canadian PIA process - 4

PIA goals:

- Build trust and confidence
- Promote awareness & understanding of privacy issues
- Ensure privacy protection is a key consideration in framing a project's objectives & activities
- Identify accountability for privacy issues
- Reduce risks
- Provide policy-makers with information to make informed policy, system design or procurement decisions

The Canadian PIA process - 5

- PIA process has four steps:

Step 1: Project initiation

- Is a PIA necessary – Is personal information being collected, used or disclosed?
- Preliminary PIA
- As design changes occur, the PIA should also be reviewed & updated

The Canadian PIA process - 6

Step 2: Data flow analysis

- Examines how information is collected & processed
- A business flow diagram to identify how information flows through the organisation, how personal information is collected, used, disclosed and retained

Step 3: Privacy analysis

- Series of questions to help identify privacy risks or vulnerabilities

The Canadian PIA process - 7

Step 4: Privacy impact analysis report

- A detailed description of the proposal's objectives, rationale, clients, approach, programs and partners
- A list of all data elements involving personal info
- A list of all stakeholders & their responsibilities
- A list of relevant legislation & policies
- Description of specific privacy risks
- Possible options to eliminate or mitigate risks
- A description of any residual or outstanding risks
- An outline of a privacy communications strategy

Benefits of undertaking a PIA

- Identifying and managing risks
- Avoiding unnecessary costs
- Avoiding sub-optimal bolt-on solutions
- Avoiding loss of trust and reputation
- Understanding & benefiting from the views and suggestions of stakeholders
- Providing a credible source of information
- Imposing the burden of proof for the harmlessness of a new technology, product or service on its promoters
- Improving public awareness
- Improving security & making life difficult for cyber criminals

Disadvantages of a PIA

Opponents probably view PIAs as

- Smacking of bureaucracy & running counter to the idea of reducing regulatory burden
- Leading to delays and additional costs in implementing a project
- Threatening their power & freedom to do whatever they want
- Imposing a burden by having to provide information to others, including possible opponents

Other stakeholders also incur costs & consume time in responding to project proposals

Should PIAs be mandatory?

What does a mandatory PIA mean?

In Canada's case, it means government institutions (but not industry) are obliged :

- to include results of their PIAs when they make submissions to TBS
- to provide a copy, approved by the Deputy Minister to the OPC
- to develop risk assessment and mitigating measures for privacy issues
- to make PIA summaries public

Institutions are expected to show evidence of

- Programs in place to inform staff & stakeholders of the PIA policy's objectives and requirements
- Formally defined responsibilities and accountabilities
- A system to report all new initiatives that may require a PIA
- A body composed of senior officers charged with reviewing and approving PIA candidates
- An effective system for monitoring compliance
- Adequate resources committed to support the PIA process

The case for mandatory PIAs

- Privacy risks are widespread
- Privacy risks provoke serious concerns and loss of confidence among consumer-citizens
- Data breaches and losses afflict both government and industry
- In the UK, the number of reported breaches & losses have “soared” since HMRC lost 25 million child benefit records in Oct 2007
- 70% of UK organisations have experienced a data breach in 2009, up from 60% in 2008
- Information systems should be regarded as (relatively) dangerous until they are shown as (relatively) safe [Raab]
- PIAs would increase awareness of the exigencies of the Data Protection Directive
- Accountability and transparency

The case against mandatory PIAs

- No need as long as existing privacy and data protection legislation is respected
- But Art 20 foresaw something like PIAs
- But the EC, custodian of the Directive, has recommended PIAs for new RFID
- Mandatory PIAs would require new legislation, esp if PIAs were mandatory for both government and industry
- Mandatory PIAs will increase the time, cost and resources needed to implement projects
- But such time and cost may be a good investment if they mitigate risks and foster trust & confidence
- A PIA process is only as good as the people involved
- Conducting a PIA may become routinised, an exercise in legitimation rather than risk management

Beyond mandatory PIAs: audits and metrics

- Audits and metrics are needed to make sure PIAs are actually carried out and properly so and where improvements can be made
- Reviewing PIA policy and its implementation helps build trust
- The ICO does not keep statistics on the use of PIAs, nor does it require entities to notify it, unlike its Canadian counterpart
- The OPC has proposed a registry of all PIAs to improve visibility, transparency, accountability

The OPC audit of PIA practice

OPC did a detailed audit of nine government departments and institutions and surveyed 47 others in 2007. It found:

- Some good practices (which it identified), but…
- 89% said they used personal info in the delivery of programs and services
- Resource shortages
- Two-thirds had no formal management framework in place to support conduct of PIAs
- Lack of a screening process to identify when PIAs should be undertaken
- Only a minority posted PIA results on their websites

The OPC audit of PIA practice (cont'd)

- Many not properly monitoring implementation of risk mitigation measures
- Some PIAs were initiated well after a project's conception or design
- Institutions were slow to address the privacy risks
- Additional training and guidance were needed
- PIAs should consider cumulative effects on privacy resulting from a project in combination with others.

Conclusions - 1

- Most people simply do not believe their personal data is safe
- There are justified fears that personal data is used in ways not originally intended, fears of mission creep, of our being in a surveillance society, of cybercriminals
- Such fears and apprehensions slow down development of e-government and e-commerce, and undermine trust
- Assuming most organisations want to minimise risks, then PIAs should be used
- Even so, many organisations are not likely to use PIAs unless they are obliged to
- Given the risks, the number & magnitude of breaches, losses and intrusions, the case for mandatory PIAs for both government & industry seems unassailable

Conclusions - 2

- But are mandatory PIAs enough?
- PIAs are typically concerned with individual projects, programs or services
- There is a need to deal with privacy implications of plans and policies that cut across many programs or services
- PIAs should also deal with information sharing
- Each project, independently assessed, might be okay, but the cumulative effect on privacy may be dangerous
- Whether PIAs gain enough traction to become mandatory remains to be seen
- Perhaps a test of strength will come when EU MS respond to the RFID Recommendation to put forward a PIA framework for consideration by the Art 29 WP

PIA handbooks

Australia

http://www.privacy.gov.au/publications/PIA06.pdf

Canada

http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp

New Zealand

http://www.privacy.org.nz/privacy-impact-assessment-handbook

UK

http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

Thank you
for your attention
☺

david.wright@trilateralresearch.com