

Privacy impact assessments around the world

Colin J. Bennett

*Department of Political Science
University of Victoria, Victoria, B.C.
cjb@uvic.ca*

<http://web.uvic.ca/poli/bennett>

Surveillance Society Conference

*December 11, 2007
Manchester, UK*



Scope of Study

- Case studies of Canada (and provinces), Australia (and states), the United States, New Zealand, Hong Kong and selected European jurisdictions, based on documentary and interview data
- Authors:
 - Robin Bayley (Linden Consulting, Victoria BC)
 - Colin Bennett (University of Victoria)
 - Andrew Charlesworth (University of Bristol)
 - Roger Clarke (Xamax Consulting, Australia)

DEFINITION OF PIAs

PIAs should:

- conduct a prospective identification of privacy issues or risks before systems and programmes are put in place, or modified
- assess the impacts in terms broader than those of legal compliance
- be process rather than output oriented
- be systematic

RATIONALES

1. Managing Risk
 1. Reputational
 2. Economic
 3. Legal
2. Improving Decision-Making

1. Managing Risk – Reputational, Economic and Legal

PIAs:

- ensure that a business is the first to find out about privacy pitfalls in its project, rather than learning of them from critics or competitors
- save money by identifying privacy issues early, at the design stage
- maintain competitive advantage (in private sector)
- avoid litigation risk and provide tangible proof of compliance with data protection law

2. A Management Tool for Improved Decision-Making

PIAs:

- bring privacy responsibility clearly back to the proponent of a proposal, where risk is best managed
- promote systematic analysis of privacy issues in order to inform debate on proposed or existing information systems, technologies or programmes
- provide credible information upon which business decisions can be based
- contribute to a culture that is respectful of customers and citizens
- build trust in electronic service delivery
- demonstrate to the public the agency's or company's commitment to privacy
- prevent "function creep"
- increase transparency

THE DIVERGENCE OF PRACTICE

PIAs Vary According to the:

1. *Level of prescription* (whether the conduct of PIAs is discretionary or mandatory)
2. *Application* (type of organisation that is expected to conduct PIAs)
3. *Conditions* (what type of initiative or circumstances trigger a PIA)
4. *Breadth of Instrument* (type or comprehensiveness of the analysis)
5. *Who completes* them (programme, privacy staff or others?)
6. *Timing* (when the PIA is conducted and if it is a snapshot or multi-staged)
7. *Process of Review / Approval* (are they reviewed externally, by whom, and to what end?)
8. *External Consultation* (with outside stakeholders)
9. *Transparency* (whether and how reports are made public)
10. *External Reviews* of PIA Processes

EFFECTIVE PIAs

PIAs are perceived to be more effective when they :

1. are Comprehensive, Flexible and Embedded
2. are Appropriately Timed and Resourced
3. entail Accountability Features

1. Comprehensive, Flexible, Embedded

PIAs are generally more *effective* when:

- They are part of a system of incentives, sanctions and review
- They are embedded in project workflows or quality assurance processes
- They are conducted within a framework which takes into account the broader set of community values and expectations about privacy
- They refer to an entire process of assessment of privacy risks rather than a statement or end-product
- The scope and depth is sensitive to a number of crucial variables: the size of the organisation; the sensitivity of the personal data; the forms of risk; the intrusiveness of the technology.
- The PIA tool is accessible, flexible and easy to access

2. Appropriately Timed and Resourced

PIAs are generally more *effective* when:

- they offer a prospective identification of privacy risks *before* systems and programmes are put in place
- when they have the potential to alter proposed initiatives in order to mitigate privacy risks
- when the individuals responsible for the PIA have good programme knowledge *and* access to multidisciplinary expertise from a variety of perspectives
 - privacy law and practice, information security, records management, and other functional specialists as appropriate

3. Entail Accountability Features

PIAs are generally more *effective* when:

- a strong advocacy role is played by the relevant oversight body
- there is external consultation with outsiders affected by the initiative
- there is transparency, and the resulting statements or reports are published
- there is a process of formal or informal external review either by central agencies or privacy oversight bodies

INTERNATIONAL OBSERVATIONS

- Mainly a feature of countries with “privacy” rather than “data protection” legislation
- No jurisdiction that has introduced PIAs has abandoned them
- Once introduced, their application spreads
- Generally, the PIA method and tool evolves, and more specialised tools emerge (e.g. electronic health systems)
- PIAs become embedded in other management processes

BOTTOM LINE?

**PIAS ARE A GOOD IDEA
Questions?**

cjb@uvic.ca