Privacy Analysis of Current Extra-National Outsourcing Practices: Focus on the PIA

March 6, 2015

Faculty of Information, University of Toronto
Stephanie Perrin

Assessing Privacy Risks of Extra-National Outsourcing of eCommunications: A research project funded by the Office of the Privacy Commissioner of Canada through the 2014-2015 Contributions program.

Is a Privacy Impact Assessment Useful?

- Started as a way of coping with e-government initiative risks: change was causing problems, there was a knowledge gap
- Regardless of media, has become a standard way of doing privacy analysis
- Hundreds of examples online, from around the world

…But do they actually contribute anything?

What is a PIA?

- Is it a risk assessment?
- What "impacts" does it assess?
- Is it a contract?
- Is it a management plan?
- Is it the same thing as a legal review?
- Is it the same as a privacy policy?
- Who does it? Who approves it?
- Who takes responsibility for it?
- Does it impact liability?

Is a PIA effective?

That depends!

- Is it scoped properly?
- Did the person(s) doing it understand the project and the environment?
- Did the drafters get the support of the organization to provide necessary information?
- Did the drafters understand the data protection requirements?
- Did they get the cooperation of security officers, and coordinate with any threat risk assessments that were done?
- Did they follow applicable guidance?

Guidance and Templates

Why did the streamlined template emerge?

- Cost of consultants
- Apparent complexity
- PIA review backlog
- Management frustration
- Streamlining
- Training issues
- Publication online

Guidance and Templates

Is a detailed questionnaire better?

- How knowledgeable is the drafter of the PIA with respect to data protection law?
- How much cooperation will the drafter get?
- How well do they know the organization?
- Is this a team effort?

PIA common problems

- Incorrect assumptions about law and legal definitions
- Scoping too narrowly….eg. in e-outsourcing, not including data contained in the email repository. The privacy risk is in the other personal data, not the authentication schemes
- Security is either too dominant or not present enough, balance is required
- Many organizations are very defensive about explaining their data maps, so basic data about what is at risk is often hard to get, and drafters may need people skills to find out what is going on.

PIA common problems

Not getting management support

- Resource requirements: a good PIA can take a year
- Plausible deniability: A good PIA can be a risk
- Fear of Access to Information and disclosure
- Impatience with approval process
- Bad news syndrome; fundamental problems with the communication of risk

PIA common problems

Not getting the data

- Need to understand all risks
- Need to understand all aspects of contract and contractor
- Need to understand all security risks and mitigations
- Need to get data about resources….will there be money to mitigate privacy issues, often deemed out of scope
- Turf war can keep information owners from cooperating
- Staff may be sensitive to lack of management support

PIA common problems

Followup and control

- Need owners for all risks
- Need the PIA to remain evergreen, not be a tickbox exercise
- Need full institutional support, cannot become a “gotcha” exercise

PIA best practices

- Follow the best guidance documents you can find, but use the template required in your jurisdiction
- Do the diplomatic work required to get cooperation and management support before your PIA drafter is in the field
- Get buy in for the project management plan to do the PIA (try finance…they hate paying for things that get messed up)
- Emphasize the positive….this is part of a risk strategy
- Get allies: legal services, security, privacy office
- If using a contractor, accompany them and check their work
- Whatever your regulatory requirements (review or approval by the privacy commissioner) try to establish good relationships, and walk them through it if possible

And remember….

This may be your first PIA, but the chances are good your regulator has seen dozens or hundreds. Don't cut corners, don't copy the other fellow's, and above all be truthful. All kinds of people can spot the spin when they get their hands on your document.