Mapping Privacy requirements onto the IT function

Part 1

Stephen Wilson

Privacy Law & Policy Reporter, Vol. 10 p11, May 2003

Executive Summary

Full and ongoing conformance with the provisions of Privacy legislation has greater impact on a business's risk management and technology management processes than often they first realise. It is tempting to believe that because privacy issues are broadly business based, they are mainly the concern of the legal department or of audit. But current catch-cries along the line that "privacy is not a technology issue" should not be interpreted to mean that privacy has no relevance for the IT function at all. There are multiple regulatory requirements of the privacy regime that directly impact most organisations' Information Security Policies, IT management functions, product/service development processes, and internal audit.

This paper presents a detailed mapping of the 10 National Privacy Principles (NPPs) onto the sorts of management processes that in most organisations are controlled by the IT function. The mapping exposes the breadth and depth of impact that Privacy compliance has on the IT function. It thus clarifies how each individual business should fine tune its processes and mobilise its IT function to satisfy the NPPs. It is hoped that such mapping can be repeated and built upon, leading to a common framework for analysing threats and risks to privacy compliance across all organisations.

The limitations of traditional privacy statements

Until recently, only government entities were formally subject to privacy regulations. But in 2000, the Commonwealth Government passed the *Privacy Amendment (Private Sector) Act*, which applies to all businesses turning over more than A$3M p.a., and to all organisations in the health sector regardless of their size.

The response of many entities to their new obligations has been to engage lawyers to produce a *Privacy Statement* defining the organisation's high level undertakings under the law. Any approach informed by legal obligations will naturally be dry and minimalist. Thus a typical Privacy Statement looks something like this:

ACME Limited shall comply with the National Privacy Principles as defined in the Commonwealth Privacy Amendment (Private Sector) Act 2000.

The only Personal Information collected by ACME is information necessary for performing our legitimate business functions. All Personal Information is collected by fair and lawful means. Personal Information is stored securely and retained only as long as it is needed for business functions. No Personal Information is disclosed to any third parties unless required under law, is necessary to perform our business functions, or ACME is requested to do so in writing by the individual.

All individuals on whom we hold Personal Information are able to view and correct or update their Personal Information, unless there is legitimate reason to deny such access.

Having a lawyer draft the Privacy Statement is of course a good idea; the Privacy laws are not to be trifled with. And the scope of most Privacy Statements is appropriately broad, since information privacy truly affects the entire business, not just IT. After all, only one of the 10 National Privacy Principles *expressly* deals with technology.

Yet the high level approach can lead to detailed security and technology management issues being overlooked. On close inspection, we see that every one of the NPPs can deeply affect a business's IT function, policies and procedures, as well as all the interfaces between IT and the rest of the business.

So while it is true that privacy affects the whole business, the IT function cannot afford to assume that privacy compliance will be managed by some other department. In order to ensure robust, long term compliance with the privacy regime, it is vital that every organisation consider how they should mobilise their IT functions in response to the NPPs.

How should the IT Function approach Privacy Risk Management?

Privacy protection is indeed a broad based business issue. Properly managed IT and security functions are not in themselves *sufficient* to ensure privacy protection – but nevertheless they are *necessary*. So it is vital that the IT Function be properly engaged in meeting the requirements of privacy legislation.

Information technology and security should strive to meet the following objectives in managing risks associated with the current privacy regime:

1. Analyse and specify in detail the organisation's privacy safeguards and information disclosure protocols. In order to ensure ongoing compliance, the level of detail has to extend beyond *what* the organisation aims to do, to specify *how* will implement its privacy safeguards.

   Privacy safeguards and protocols may be written up within the organisation's

existing IT and security procedure framework, but a distinct "Privacy Management Strategy" is a better idea, to help concentrate the effort.

2. Be able to demonstrate to auditors and others that the organisation has *systematically and proactively* considered its privacy position, and that it has the means to continue complying with the Act, rather than merely pass a short term privacy audit.

3. Ensure that the organisation looks beyond the more obvious technological issues like access control and encryption, to cover information architecture, systems design, design review and internal audit.

4. Ensure that the organisation's product/service development processes (as applicable) are fully informed by privacy protection requirements.

5. Obtain senior management sign-off on the organisation's documented position on privacy safeguards, as adjudged to be reasonable and practicable for the business.

The scope of Privacy Risk Management

A comprehensive framework for privacy risk and technology management must consider a range of issues. The Privacy Management Strategy or other documentation should cover the following:

- **The nature of the business and industry sector** in the context of privacy protection. The organisation should construct its own framework in which to make robust, defensible decisions on issues like what personal information is required to support the business, what if any *sensitive* information is required,[1] which information is collected manually, automatically and by acquisition from third parties, and what reasonable assumptions can be made about their users' consent to information usage and disclosure.

- **Interpretations** of the qualities of *reasonableness* and *practicality*, called for throughout the Privacy Act. The onus in the current regime is on organisations to implement measures that are "reasonable" under their particular circumstances, and for them to decide what sorts of actions are "practicable", especially with respect to obtaining consent for information to be used and disclosed.

  The light touch regime allows plenty of room for judgment in assessing these qualities, but significant responsibility attaches to this flexibility. Privacy auditors will expect management to have analysed the issues and documented their

[1] "Sensitive" information is defined as that which either relates to race, ethnicity, religion and so on, or which is health related. The Privacy Act and its private sector amendment calls for special treatment of sensitive information.

decisions in advance.

Standards for reasonableness might in some cases be drawn from industry norms or Codes of Practice where available. Otherwise, they can be determined from first principles by undertaking a formal Threat & Risk Assessment (TRA) and/or Privacy Impact Assessment (PIA).

- **All personal information collection methods** should be enumerated, together with the organisation's rationale for needing the information, and the appropriate controls associated with each method. It is especially important to analyse and document the less obvious types of collection such as transaction histories and audit logs, which are often collected automatically.

  Personal data collection can be considered under five categories:

  1. ***Overt collection*** via application forms, web forms, call centres, face-to-face interviews, questionnaires, warranty cards etc.
  2. ***Automatic collection*** especially via audit logs and transaction histories.
  3. ***Generated data*** includes evaluative data and inferences drawn from collected data, for the purposes of service customisation (e.g. buying preferences), business risk management (e.g. insurance risk scores from claims histories) and so on.
  4. ***Acquired data*** is that which has been transferred from a third party, with or without payment for the data, including cases where personal information is acquired as part of a corporate takeover.
  5. ***Ephemeral data*** is a special category of automatic or generated data, produced as a side effect of other operations. Ephemeral data is reasonably presumed to be transient but can be inadvertently retained. For example, some systems prompt users for pre-arranged challenge-response information – classically their mother's maiden name – when dealing with a forgotten password. The data provided can be left behind in computer memory or logs, or even scribbled on a sticky note by a help desk operator, and represents a major privacy breach if it is not protected from unauthorised parties.

- **Design and review processes** must explicitly check for compliance with the NPPs, especially around data collection forms, database design, and audit logging. If the organisation has a formal product or service development process, then all stakeholders engaged in that process should be aware of privacy requirements so that design decisions are well informed.

  For example, ad hoc changes should never be made to web forms which gather personal data, without referring to the business need for any new information to be collected. Demographic data collection can be particularly troublesome, because of the temptation to ask for things like age, gender and locale to support sales and marketing functions. But under the privacy regime, no such data may

be collected without there being an express business need for it, and appropriate consent mechanisms and controls being in place. The Privacy Management Strategy, by documenting the nature of the business and the types of information it requires, provides a robust common framework within which to make robust defensible design decisions.

- **Certain standard items in most Security Policies and Procedures** directly relate to privacy protection issues – especially data archiving, data destruction, access controls and encryption. Security documentation must be written and reviewed where necessary, paying heed to the new privacy regulations.

- **Formal protocols for disclosing information to third parties.** The Privacy Act allows for information to be transferred to a third party under certain circumstances. It is generally expected that the third party will itself not subsequently disclose the information to further parties. To properly handle these conditions, formal protocols should be developed which anticipate the scenarios where information can be disclosed, and the controls which will be put in place to ensure compliance with privacy regulations.

- **Architecture** of information systems may need special attention to meet privacy requirements. Particular examples of architectural issues under the privacy regime include:

  - Where information is held on disparate or distributed systems, it is essential that a definitive record can be produced in a timely manner in response to a customer request, and that changes to that record can be promulgated back into all the organisation's systems in the event of an update.
  - Where data has been backed up or duplicated, the requirement to destroy personal information when no longer needed can be complicated.
  - Audit logs can constitute a rich source of personal information, but logging functions have not historically been engineered to allow ready access of individual records. Such access can be necessary under the privacy regime, to permit disclosure, updates, destruction and so on.

- **Outsourcing** of information systems operations or other IT functions can lead to personal information being held outside the organisation. The inter-relationships between privacy regulations and outsourcing are complex, somewhat ambiguous, and still under active consideration by the Privacy Commissioner.[2] In the current climate, organisations will benefit from tackling relevant outsourcing issues proactively, and with regard to their own business circumstances. The organisation should critically review the privacy policy and privacy protection measures of their outsourcer.

[2] See for example the Privacy Commissioner's submission to the Senate Inquiry into the Commonwealth Government's IT Outsourcing Initiative, at http://www.privacy.gov.au/publications/subout.pdf.

Documenting a full Privacy Management Strategy

The concept of a full Privacy Management Strategy goes beyond the typical Privacy Policy Statement that many organisations have already developed. The major differences are as follows:

Privacy Policy / Statement	**Full Privacy Management Strategy**
Presents high level business objectives.	Details the characteristics of the business and its industry sector, to underpin judgments of what is reasonable and practicable when interfacing with customers and other users.
Generally emphasises *what* the organisation will do under the Privacy Act.	Specifies *how* it will maintain compliance
Public document, usually addressed to non-technical stakeholders, mainly interested in how the organisation's privacy safeguards affect them personally.	Company Confidential document, intended for internal staff (especially though not exclusively the IT Function) or auditors.
Generally technology neutral, covering broad based management issues.	Has a significant technology component, specifically in order to inform and guide IT management, IT procedures, systems design, and security.

A suggested table of contents

A Privacy Management Strategy might be written according to the following structure. The suggested structure is generic and would be modified to best suit the specific requirements and issues of the business.

1. The Nature of the Business *A reasonably in-depth commentary on the nature of the business and the industry sector, to set the scene for organisational responses to the privacy regime.*	– Individuals affected by our business – Third parties with whom we deal – Cross border parties with whom we deal – Overview any internal Product/Service development processes – Applicable Privacy Codes of Practice – Other applicable laws & regulations – Anticipated risks of personal injury resulting from conduct of the business
2. Information to support the Business *A thorough catalogue of the types of information needed to support the business, and how it will be collected and managed.*	– Types of information in general required by the business – Types of personal information in particular required by the business – Collection methods [as applicable]

	o manual o automatic o generated o acquired o ephemeral – Specific needs for *Sensitive* information – Specific needs to share information – Practical issues around the ability to obtain consent to use & disclose – How information ages in the context of the business – How information quality will be maintained
3. Organisational responses to Privacy *An overview of how certain organisational units and common processes—especially those related to IT – are to be managed or modified in response to the privacy regime.*	– The IT function – Security Policy & Procedures – Customer relations – Product/Service Development Lifecycle – Internal audit – External audit
4. Information Sharing *Specific issues concerning any anticipated sharing of personal information with third parties.*	– Disclosure protocols – Expectations of third party Privacy Policy – Existing regulatory protections in cross border locations, as applicable – Projected regulatory protections in cross border locations, as applicable – Expectations as to how third parties will be held to their Privacy Policy and/or regulations as applicable
5. Architectural Considerations *High level requirements and design issues affecting different sub-systems in the organisation's information systems architecture, as applicable.*	– Database design, including the ability to annotate changes and consent issues – Database update methods and quality controls – Audit logs, especially the ability to locate, extract and delete personal information relating to a given person – Access control – Encryption – Authentication – Recording of consent – Use and assignment of identifiers
6. Special Issues *As applicable.*	– De-identification standards and protocols – For banks (esp. Basel II requirements) – For health organisations – For insurance & superannuation companies – For non-profit organisations – For direct marketing companies