Lockstep Consulting
ABN 59 593 754 482
Contact: swilson@lockstep.com.au

Don't let privacy take IT by surprise

Stephen Wilson
Online Banking Review No. 4

Despite being hyped as the biggest compliance issue since Y2K, Australian privacy legislation has not had widespread impact on how banks run their businesses. Most financial institutions have always been sensitive to their customers' privacy, and to that extent were well prepared for the Privacy Amendment (Private Sector) Act in 2000. Furthermore, any European bank with offices in Australia, and any merchant bank dealing routinely with institutions on The Continent, would have been aware of the tough European Union privacy regime.

The position of "Chief Privacy Officer" is increasingly common overseas. Australian businesses have typically tasked their compliance or legal functions with managing their privacy obligations. Most companies have a solid understanding of the legal technicalities of the Privacy laws; they have written compliance statements, established privacy complaint handling procedures, and in some cases adopted industry specific privacy codes of conduct.

But research is starting to show that not many IT departments have come to grips with the full meaning of privacy compliance for how institutions handle and process information. Few IT managers appreciate how the potential ramifications of privacy go far beyond security and confidentiality, to impact on database design, architecture, web design processes and audit.

It is important for IT departments to look into the Privacy Act for themselves, and for the organisation's legal and technology functions to work closely together. The implications of consent management on database design in particular need to be understood by all, so that non-technologists don't make false assumptions about what CRM systems are actually capable of.

Many of today's new regulatory regimes in fact have subtle and far-reaching implications for the enterprise IT function, especially when they change the way customer information is handled. It is imperative that IT managers understand the ramifications of each new regime and have a plan of action to meet their new

responsibilities. Analysing our privacy regulations is a great way to bring an organisation's technology and compliance arms together, so that technical details stop falling through the cracks. There are plenty of lessons for banks planning for Basel II in the way their IT shops support the privacy regime today.

In the current environment, businesses are well advised to take a "holistic" view of Corporate Governance. Thus IBM chairman Lou Gerstner famously said in 2000 that "privacy is not a technology issue". True enough: good privacy management definitely calls for a multi-disciplinary approach. But the well-meaning slogan does not mean that IT management is entirely off the hook!

Technologists can be forgiven for thinking the Australian Privacy Act doesn't much relate to them. After all, of the 10 National Privacy Principles written into the legislation, only one of them relates directly to data security. The other nine NPPs appear to be customer relations matters (see table).

But on closer inspection, all NPPs have to do with data management and therefore have direct implications for information technology.

For example, NPP 1 (Collection) requires organisations not to gather personal information unless it is needed to run the business. NPP 1 is easily broken if web forms are designed in an ad hoc manner and without proper sign-off by legal. Many web masters asked to create a client enrolment form might think it reasonable to collect gender, date of birth and/or demographic details while they're at it. But if such information isn't truly needed by the business, then the organisation is breaking the law by asking for it.

NPP 6 (Access and correction) gives customers the right to see what personal information a business holds on them, and to request that records be amended or deleted. Yet organisations can struggle to pull together a complete record for a given person, and can be surprised by the extent of personal information contained in audit logs.

Remember that the Privacy Act doesn't care where personal information comes from. Under the act, the collection of information is not restricted to customer details provided explicitly in forms and questionnaires; collection also covers transaction histories, as well as evaluative information created within the organisation, such a credit risk assessments. So much of this information is generated and stored in disparate systems that meeting the requirements of NPP 6 can be extremely challenging. All businesses must do their own stock-take of the types of information they gather and hold, and what can be done to collate, update or destroy that information should the need arise.

So the privacy regime has deep and somewhat surprising implications for any organisation's IT function. Technologists might be tempted to think that strong encryption and access controls are all that's required. But architectures, databases and audit logs can all undo your compliance unless they are coordinated by a privacy management function alert to the subtleties of modern information systems.

A Privacy Management Strategy is the best way to tackle this particular compliance issue. And you may be surprised by what you learn about your compliance posture in general, when everything about your business today tracks back to the way information is managed.

NPP 1	**Collection:** You must not collect personal information if it's not necessary to the running of the business
NPP 2	**Use and disclosure**: You must not disclose information without consent, unless disclosure is related to the reason for collection
NPP 3	**Data quality**: You must keep personal information records accurate and up-to-date
NPP 4	**Data security**: You must take reasonable steps to safeguard information
NPP 5	**Openness:** You must disclose your privacy policies, the types of personal information you hold, and why
NPP 6	**Access and correction**: You must provide people with access to personal information you hold on them
NPP 7	**Identifiers:** You must not re-use government-issued identifiers such as drivers licence numbers and Tax File Numbers
NPP 8	**Anonymity:** Wherever possible, people should be given the option of dealing anonymously with your organisation
NPP 9	**Transborder data flows**: You must take reasonable steps to ensure that offshore entities have controls equivalent to the Privacy Act
NPP 10	**Sensitive information:** You must take special steps when handling information relating to gender, religion, race, sexuality and so on.

Table: The National Privacy Principles, briefly explained

About the author

Stephen Wilson is a leading international authority on identity management and information security. In early 2004 Stephen established Lockstep Consulting to offer independent advice and management consulting on security strategy, online authentication, e-business risk management, and privacy. Contact Stephen at swilson@lockstep.com.au.