Wigley & Company

BARRISTERS and SOLICITORS

Privacy Implications for Information Technology

Presentation to Corporate Lawyers
September 2006

IT projects, ranging from websites and online trading through to protection of computerised databases, often raise privacy issues. We summarise the issues that typically arise, and highlight the need for privacy issues to be handled carefully, in a way which integrates appropriately with other IT project requirements.

Introduction

IT projects often involve the handling of personal information and so they frequently raise privacy issues. Security (an ever present feature of IT projects) is integrally related to privacy[1], yet the privacy aspects are often largely overlooked or left to the last minute. Or the opposite can happen: too much focus on privacy (and compliance beyond what is required) to the exclusion of other project needs. Either can lead to problems, including project failure.

IT projects of course raise numerous issues. It often happens that a stakeholder with a keen interest in one of those issues will inappropriately skew the focus of the project so that various issues such as technical, commercial, privacy, legal, etc are not adequately balanced. The stakeholder might take a "silo" approach to his or her issue, without regard to its impact on other project needs. This can make, for example, privacy compliance either slacker or more stringent than is appropriate. Almost always, 100% solutions on each issue (eg, a solution that provides 100% security and privacy protection) are not possible and some compromise is needed. The idea is to get the balance right. That's something that great project managers and owners do.
While calling for sufficiently high standards and protection of information, the Privacy Act is relatively facilitative and fluid in this respect.

[1] We have dealt extensively elsewhere with security requirements in relation to IT projects and will not go into detail here. See our paper "*Legal Compliance and IT Security*" at: http://www.wigleylaw.com/assets/_Attachments/LegalCompliianceAndITSecurity.pdf.

Privacy Act and Related Legal Obligations

Often, the talk is only about the Privacy Act. Yet there are other legal issues.

The Privacy Act is about personal information, that is, information about individuals. Those implementing IT projects often handle information outside the Act (eg, information specific to a company which is not covered by the Act)[2]. There are other regimes which overlap with Privacy Act territory and deal with information outside the ambit of that Act. For example, there is:

- the law as to confidentiality;
- the developing tort of privacy;
- the law of negligence (that might kick in where an organisation negligently releases confidential information); and
- the law of contract.

We deal with these in more detail in the following papers:

- "*Confidentiality and Restraint of Trade: Practical Issues*"[3];
- "*Confidential Information Breaches can be Difficult to Prove*"[4];
- "*Mike Hosking and Naomi Campbell Develop Privacy" and "Confidentiality Law*"[5]; and
- "*Legal Compliance and IT Security*" [6].

[2] Although business and corporate information can sometimes raise details about individuals in such a way that the Act does apply.

[3] http://www.wigleylaw.com/ConfidentialityAndRestraintOfTradePracticalIssues.html

[4] http://www.wigleylaw.com/ConfidentialInformationBreachesCanBeDifficultToPr1.html

[5] http://www.wigleylaw.com/HoskingAndCampbell.html

Projects often consider only Privacy Act issues, when they should consider wider confidentiality and privacy concerns as well.

However, compliance with Privacy Act obligations, as though they apply to *all* types of information, often is sufficient to minimise risk in relation to non-Privacy Act risk areas. Each situation of course will depend on its own facts. Say, in a contract, an organisation promises to keep information 100% secure and fails to do so. It may be liable to the affected person, when IPP5 in the Privacy Act (which we deal with below) would otherwise allow some leeway.

Storage and Security of Personal Information (IPP5)

Keeping databases secure is a big issue, highlighted for example by:

- The well publicised accidental or hacked releases of databases internationally and locally;
- The struggles the banks are having with internet banking: when the banks recommend that internet banking should not take place at internet cafés, it's clear there are big problems.

The Privacy Act revolves around 12 Information Privacy Principles. IPP5 is a key issue for IT projects. It requires an agency that holds personal information to ensure that:

> "*(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:*
>
> *(i) Loss; and*
>
> *(ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and*
>
> *(iii) Other misuse; and*
>
> *(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.*"

We have dealt extensively elsewhere with security requirements in relation to IT projects and will not go into detail here. See our paper at footnote 1 above and also our paper *"Ensuring your Legal and IT Security"*.[7] There is also very helpful guidance in the Privacy Commissioner's commentary on the Health Information Privacy Code 1994, available for purchase from the Commissioner's office. See in particular the commentary under Rule 5. Health Information requirements mirror what agencies should do about particularly sensitive information generally. See also our papers on *Electronic Health Records*.[8]

The first key point to emerge from IPP5 is that the agency is required to protect the information by such security safeguards **as are reasonable in the circumstances**. There is a judgment call here, of course. The more sensitive the information, the higher the security barriers, and vice versa. With IT projects, there will almost always be some trade-off: the question is, how much? This does enable some trade-off between (a) ease of accessibility and functionality, and (b) protection of information. There is an implicit recognition that, in some instances, it will be possible for a hacker or someone else to get into the information, even though steps must be taken to minimise (but, not necessarily eliminate) this risk. Applying proper security standards in an IT project context (eg, by applying AS/NZ17799 Standards) will often produce the same level of protection as is required in a privacy context. Sometimes, the sensitivity of the information is so great that a particular IT solution cannot be used and a very different alternative must be found (IT or otherwise).

The required level of protection of the information, refers to every kind of potential access to the information including internally in the organisation, by third parties accessing the information for whatever reason (such as providing services), and access by external parties (such as customers, hackers, etc). This raises physical, operational and technical security issues. A couple of examples:

[6] See footnote 1

[7] http://www.wigleylaw.com/assets/_Attachments/EnsuringYourLegalITSecurity.pdf.

[8] http://www.wigleylaw.com/mainsite/ElectronicHealthRecords.html

- Sufficiently identifying external parties that seek to access information - in the lingo of the IT world: *authentication*. We deal with this below.

- Provision of information to a third party supplier in connection with the provision of a service by that third party to the agency. For example, an agency could outsource its data operations to a third party provider. IPP5(b) requires the agency that initially holds the information to do everything reasonably within its power to ensure there is no unauthorised use or unauthorised disclosure of the information when a third party supplier is involved. In our experience of IT projects, this is an issue that's often overlooked. It is not enough just for the agency holding the personal information to allow some service provider to have access to that information without imposing further restrictions (this often happens). The agency must go further and do everything reasonably in its power to prevent unauthorised use or unauthorised disclosure. It might do that technically (eg, by minimising access to the database, requiring sufficiently robust authentication, etc). Sometimes it can't go that far in view of the level of access that the third party has to have to the information. Therefore, it will be relying upon, for example, a contractual commitment from that third party to ensure that the principles of the Act, including IPP5, are met. Often, a contract is not enough. The initial agency may need to go further, such as by monitoring, ensuring sufficient process is in place at the other agency, etc. The health sector is an example of where we often see inadequate compliance with this obligation under the comparable provision in the Health Information Privacy Code.

Online Issues

Websites raise many privacy issues. It is common to see a hyperlink at the foot of a front page of a website, which links to a privacy policy. Those statements often pivot around meeting disclosure obligations in the Privacy Act (eg, IPP3) and authorising wider use and disclosure of information than is otherwise permitted by the Act (eg, IPPs 10 and 11).

IPP3 requires that an agency takes "*such steps (if any) as are, in the circumstances, reasonable to ensure that*" the individual concerned is aware of matters such as the purpose for which the information is being collected, intended recipients of the information, the person's rights of access etc to the information, and so on. IPPs 10 and 11 limit the ability of the agency to use and disclose the information to only the purpose for which it was collected (or a purpose that is directly related to that purpose).

There are some exceptions to this. An important one is that the agency "*believes, on reasonable grounds …*" that the use or disclosure is authorised by the individual concerned. For example, a business that has collected information for one purpose may want to use it for unrelated marketing purposes (and a public sector agency may have a similarly wide purpose in mind). To do this, it will generally need to show that reasonable steps have been taken to secure the individual's authorisation.

A privacy policy will often be drafted to deal with these issues (although the wording of the policy is decidedly mixed on many websites). In many, if not most situations, it must be highly debatable whether, having this information contained in a web page to which there is only reference at the foot of a home page, is sufficient to meet the statutory obligations. Something that involves stronger linking between the affected person and the policy would generally be needed to meet Privacy Act requirements.

It's useful to start from an offline benchmark: signed up acceptance of a privacy policy where the relevant words are closely linked to a handwritten signature. This is powerful. To replicate this online is clearly more difficult. The best solution in practice will be a "*click accept*" of the privacy statement (where the policy is sufficiently linked to *"click accept"*). In higher risk situations, however, there is an inherent difficulty in view of the authentication issues noted below. Each situation needs to be assessed based on the issues and concerns it raises.

The *"click accept"* privacy policy should be set up carefully so that the *"click accept"* is closely linked to the words in the privacy statement (ideally highlighting particular aspects of the statement including specific proposed uses of information rather than some generic wide-ranging authorisation).

Important and unusually onerous privacy requirements can be lurking and buried amidst the detail of a privacy policy. That might not

be compliant either. The law of contract raises comparable issues in relation to onerous terms: see out limitation of liability paper at para 5.[9]

This issue runs in parallel with online acceptance of contracts. That raises similar issues and the two aspects (contract formation and privacy) can generally be treated together, although the issues don't entirely overlap. This is an illustration of the point that privacy does not reside in its own silo, unaffected by other issues.

In dealing with IPPs 3 (disclosure of information), 10 (limits on use) and 11 (limits on disclosure), we highlighted the Act's reference to doing what is reasonable. In other words, 100% certainty is not always required. Whatever is reasonable in the circumstances is appropriate. Hence a *"click accept"* approach, if well constructed, will often be sufficient to meet the needs of the Act, even though it may not be a perfect solution. For ultra-sensitive information it may not be enough. One of the reasons for this is the authentication issue dealt with in the next paragraph.

Authentication

Increasingly important for evidential purposes and privacy purposes, is the issue of authentication, that is, confirming that the person presenting as Joe Bloggs is in fact Joe Bloggs. We go into more detail on this issue in our paper "*Ensuring Your Legal and IT Security".*[10] Someone *"clicking accept"* on a website, even if supported by evidence such as user name and password, digital certificates etc, proves only that someone (probably, but not necessarily, Joe Bloggs) is presenting as Joe Bloggs. This has less evidential strength than, for example, a handwritten signature. This is a point that is often overlooked when authentication models are implemented; it arises in a variety of guises ranging from low level authentication where there is no use of additional evidence such as PIN number through to high level authentication, such as username/password variants.

Unique Identifiers (IPP12)

There is a trend towards commonality of approach and common use of platforms and systems between agencies. Cross-agency use in online transactions of the same keys such as username/password (in Privacy Act lingo, *"unique identifiers"*) becomes an issue. This raises "*Big Brother*" concerns. IPP12 is designed to cover this. It restricts the ability to use unique identifiers between agencies. Unlike many of the other IPPs, it is not possible to get the individual's authority to override the application of IPP12, which heavily restricts cross-agency use of unique identifiers.

Interestingly, there is some sign of a change of mood on the international scene away from the *"Big Brother"* concerns towards the cross-agency use of unique identifiers. This is in part driven by recent terrorism events. Also, cross-agency use of unique identifiers does have some privacy-enhancing features which counter-balance negative concerns.

Privacy Impact Assessments

The Office of the Privacy Commissioner has produced guidelines for privacy impact assessments (PIAs) which are very useful. This is a comprehensive model to enable privacy issues to be assessed, which reflects what should happen in each situation, however large or small. Large infrastructure projects often call for comprehensive privacy input. From our experience it is critical that the privacy impact assessment meshes with commercial, policy, technical, security, legal and other considerations. A PIA, handled incorrectly, in our experience, can end up treating privacy as a "silo" issue. It often happens that, in an imperfect world where there needs to be co-ordination and some compromise, this does not happen. Great privacy specialists, and IT project managers and owners, will balance and manage the competing tensions.

International

By its nature, the online world frequently raises international issues including cross-border transfer of information. Depending on the circumstances, a project may need to assess the privacy impacts in another country (although typically where a number of countries are involved, the cost of making a

[9] http://www.wigleylaw.com/assets/_Attachments/LimitationOfLiabilityAndRelatedIssues.pdf

[10] http://wigleylaw.com/assets/_Attachments/EnsuringYourLegalITSecurity.pdf

comprehensive assessment will be too high). To ensure compliance, another country may require more stringent standards to be applied in New Zealand than are necessary under the Privacy Act, and may even call for changes in our legislation to accommodate cross-border transfer of information.

Wigley & Company is a long established specialist law firm. Our focus includes IT, telecommunications, regulatory and competition law, procurement and media/marketing. With broad experience acting for vendors and purchasers, government agencies and corporates, Wigley & Company understands the issues on "both sides of the fence", and helps clients achieve win-win outcomes.

With a strong combination of commercial, legal, technical and strategic skills, Wigley & Company provides genuinely innovative and pragmatic solutions.

Wigley & Company
Barristers & Solicitors
Level 7, 107 Customhouse Quay
P O Box 10842
Wellington
info@wigleylaw.com
Tel: 04 472 3023
Fax. 04 471 1833

We welcome your feedback on this article and any enquiries in relation to its contents. This article is intended to provide a summary of the material covered and does not constitute legal advice. We can provide specialist legal advice on the full range of matters contained in this article.