Outsourcing/offshoring risks

PL&B International takes a brief run through some of the key privacy risks involved in outsourcing relationships.

CONFLICTING NATIONAL LAWS

Companies offshoring their processing activities need to assess the local laws of the country they are planning to outsource to. Although the focus with data protection - especially in the European Union - is on whether the country has adequate privacy legislation in place, businesses also need to consider whether national laws might actually work against their own privacy policies by enforcing the disclosure of customer/staff data.

A current example is concern over the outsourcing of data from Canada to the US. The Privacy Commissioner for British Columbia recently launched an investigation after concerns were raised that US authorities might be able to access personal data that is outsourced to US-based service providers (see cover story).

SYSTEMS TESTING

This is an often overlooked area and especially relevant for those companies thinking of outsourcing their IT development functions. IT service providers will often request live customer data in order to test out new systems and applications. Like all data processing activities, if the relevant data protection controls are not in place, there is the potential for serious compliance gaps to occur.

As IT development is an area which does not generally involve transferring vast swathes of personal data, the data protection implications can easily be neglected when companies draw up their outsourcing contracts.

Although based on compliance with the UK Data Protection Act, the British Standards Institute (BSI) *Guidelines for the use of Personal Data in System Testing* provide some useful advice on the instructions that service providers will need to follow (see www.bsi-global.com).

TERMINATING CONTRACTS

When an outsourcing contract comes to the end of its lifecycle, or your business intends to terminate its relationship with a service provider, have considerations been made over what will happen to any personal data that is still in the hands of the service provider? Does the outsourcing contract have provisions ensuring that the data will either be destroyed or transferred back to the data controller, and how will this be achieved?

AUDITING/SELF ASSESSMENTS

Obviously for a company that has numerous outsourcing relationships, full blown data protection audits across the board will be a costly exercise, especially when service providers are located overseas.

Businesses need to assess the risks of each relationship and consider what level of detail their auditing or assessment processes should involve. For high profile and high risk agreements - such as outsourced call centre operations or HR processes - a more robust approach will be necessary. If budgets are tight, then instead of a specific privacy audit, compliance departments could consider 'piggybacking' data protection onto the overall operational assessment of the service provider.

For lower risk relationships, a less costly, although less effective, alternative is to send out self-assessments to service providers which can then be followed up more closely if any compliance gaps are identified.

RENEGOTIATING CONTRACTS

Large organisations may have long standing outsourcing relationships that pre-date the introduction of privacy laws or their own data protection policies. While companies are now writing data protection clauses into their service provider contracts, older outsourcing contracts can be overlooked. Companies such as Kodak have taken a very proactive line on this issue by renegotiating all their processor contracts so that privacy and security controls are included.

Part of the problem is in actually identifying where the contracts are located. In companies that handle procurement centrally, this will be an easier process. It gets more complex in large organisations where procurement is split between business units or corporate groups.

DUE DILIGENCE ON CONTRACTS

Data protection experts argue that while businesses generally make sure that they satisfy all the necessary legal requirements, outsourcing contracts can often lack sufficient detail on the specific processes that will be taking place. Transferring liability to the outsourced processor may cover businesses if a privacy incident occurs, but it will not protect them against adverse publicity and damaged reputation.

Businesses need to be very clear on the instructions they give to their service providers. Spelling out the precise nature of the outsourcing relationship will let the vendor know exactly what their responsibilities are. The tighter the instructions, the less chance there is of something going wrong.

STAFF AWARENESS/EDUCATION

This is probably not the greatest offshoring risk, contrary to some of the scare stories you may have come across in the media. Companies that have outsourced to India, for example, have reported that staff tend be highly motivated, willing to learn and abide by company policies.

But it is not an area businesses can afford to ignore. Many favoured outsourcing destinations do not have privacy laws and therefore staff may have a low cultural understanding of the issues.

US outsourcing, continued from p.3

sensitive personal information be promulgated and enforced if the illegitimate access to computer files were to occur in an offshore company?

- How will US companies be able to prevent overseas firms from subcontracting the work to other companies who then subcontract it to yet others?

Despite these concerns, the Privacy Rights Clearinghouse brief did suggest that the majority of US companies that hire offshore companies to handle data containing sensitive personal information will establish contracts to attempt to ensure that such data is processed in a secure environment with proper information-handling practices. And it also acknowledged that media reports on several offshore companies have described security practices that far exceed the privacy protection strategies of many US businesses.

Mixed into the apparent angst over the loss of privacy is the worry of US politicians about outsourcing of US jobs - including jobs involving the processing of personal data. The *Economist* magazine reported that Democrat candidate John Kerry has railed against "Benedict Arnold" bosses who betray their workers by shipping jobs abroad, and that Kerry has also promised that US companies will lose tax breaks if they send jobs offshore.

The same magazine reported fears in the India's booming IT sector because of one small part of an omnibus spending bill passed by the US Senate in January. The legislation would have the effect of banning some departments of the federal government from outsourcing work to poor countries - only a minor hit to the Indian economy, but one that could become more significant if US state governments were to follow suit.

US DOUBLE STANDARDS?

But it seems that not only officials in the US are concerned about offshore outsourcing. The newest twist in the tale is the growing concern about outsourcing to US companies because of the implications of the US Patriot Act, legislation passed shortly after the September 11th terrorist attacks. In May, David Loukidelis the Privacy Commissioner for the Canadian province of British Columbia (BC), announced that he would be investigating the implications of the Patriot Act on the personal data of BC residents outsourced to US-based service providers.

A background paper prepared by Loukidelis's office notes that all US companies and their affiliates are subject to the Patriot Act. It means that the personal details of BC citizens outsourced by local authorities to US service providers could be accessed by the US Federal Bureau of Investigation. Furthermore, if a US-based service provider were ordered to produce personal information pursuant to the Patriot Act, it would then be prohibited from disclosing the existence of that order.

The newest twist in the tale is the growing concern about outsourcing to US companies because of the implications of the US Patriot Act, legislation passed shortly after the September 11th terrorist attacks.

However, the Patriot Act runs headlong into British Columbia's Freedom of Information and Protection of Privacy (FOIPP) Act. The Act requires every public body in the province to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorised access, collection, use, disclosure or disposal.

Loukidelis has received complaints that outsourcing contracts giving US-based companies access to personal data controlled by public bodies in British Columbia could violate the FOIPP Act because of the reach and effect of the Patriot Act.

Loukidelis therefore has announced a review of implications which will examine the following questions:

1. Does the Patriot Act permit US authorities to access the personal data of British Columbians that is, through the outsourcing of public services, in the custody or under the control of US-based service providers? If it does, under what conditions can this occur?

2. If it does, what are the implications for public body compliance with the personal privacy protections in the FOIPP Act? What measures can be suggested to eliminate or appropriately mitigate privacy risks affecting compliance with the FOIPP Act?

Interestingly, the complainant in the BC case is also linked to employment issues. One example is the court challenge launched by the BC Government and Services Employees Union to proposed outsourcing of functions connected with the administration of BC's public health insurance plan.

The questions being asked by Loukidelis about the implications of the Patriot Act for British Columbia's data protection legislation are relevant for data protection authorities in other jurisdictions. Will the Patriot Act conflict with their data protection laws? These questions are part of the larger question of the role of companies as providers of information to satisfy the alleged security interests of states.

A further, more troubling issue, also arises with the Patriot Act. Does it attempt to extend its provisions about secret warrants and gag orders to US service providers operating entirely outside the US? The possible attempt to give the Act extraterritorial reach would be extremely troubling for most other states, since US companies operate around the globe.

CONCLUSION

In the United States, the outsourcing issue can only gain further momentum, particularly in this election year. However, one suspects that the main concern of politicians about outsourcing is loss of US jobs, not the potential for loss of privacy. At the same time, other countries have ample reason to prepare for a confrontation over the possible extraterritorial extension of the Patriot Act.