



## **Business Risks of Cross-Border Transfers of Personal Information to the United States**

As a Canadian, ask yourself these questions:

“Would you like your personal information reviewed by a U.S. law authority, say the FBI?”

“Would you like your purchasing habits, your medical information, your resume, accumulated and accessed by US government agencies?”

If these questions make you feel uneasy, you are not alone. According to a survey, published in June 2005, and conducted by EKOS Research Associates on behalf of the Privacy Commissioner of Canada, 64% of Canadians have serious concerns about companies transferring their personal information to the US.

So, as a Canadian, ask yourself this question:

“Should an organization be obligated to tell you when your personal information is going to be transferred to the US?”

Or go even further:

“Should an organization obtain your consent before transferring your information to the US?”

If you answered yes, you are not alone. The same EKOS survey found that 73% of Canadians thought it was of high importance that organizations inform them prior to transferring their information to the US. But the highest percentage, 84%, wanted an organization to obtain their consent prior to transferring their information to a foreign country, including the US.

The Office of the Privacy Commissioner of Canada has repeatedly stated, at the very least, a company in Canada that outsources

# NYMITY

information processing in this way should notify its customers that the information may be available to the US government or its agencies under a lawful order made in that country. In fact, if you are an individual residing in British Columbia, Canadian or non-Canadian, you have legislative protection that the personal information you provide the BC government will not be accessible by US law authorities. This law, a privacy law called *Freedom of Information and Protection of Privacy Act* ("FOIPPA"), extends to all BC government agencies and their 3rd-party suppliers.

## **Business Risk**

Businesses in Canada are looking at this issue seriously. Mainly because:

- companies that provide outsourcing services to a BC government agency, or in many cases any Canadian or provincial agency, must locate outsourced personal information in Canada and takes steps to ensure it cannot be compelled to release the information to the US government authority;
- outsourcing firms that provide services to risk-averse industries, say banking and insurance, are receiving pressure from their customers to keep data in Canada;
- all companies that transfer personal information to the US, either to their head office, to an affiliate, or through an outsourcing relationship, must answer the question: "What are our business risks related to transferring personal information to the US?"

Some examples of the impact this issue has had on Nymity's customers include:

- moving data centres from US locations to Canada;
- changing ownership of the Canadian subsidiary from US to UK, such that US officers couldn't compel the company to disclose information residing in Canada to US authorities;
- a US-based firm not bidding on a contract, as it would be cost-prohibitive to move their data centre to Canada, in

# NYMITY

keeping with contract requirements;

- winning a 14 million dollar contract because their data centre is in Canada;
- creating sales and marketing strategies to capitalize on the fact that they are a Canadian company and all information resides in Canada;
- the Canadian subsidiary of a US owned company creating a datasheet to explain why the USA Patriot Act does not apply as their Canadian operations are completely independent and out of the reach of the US head office;
- changing privacy policies in hopes that providing notice to consumers of their practices related to cross-border transfers of personal information will make them compliant with privacy laws in Canada;
- conducting audits of their service providers to ensure they are not using US-linked sub-contractors;
- updating contracts with service providers;
- updating customer contracts to provide notice of any cross-border transfers of personal information.

## USA Patriot Act

Why are business risks increasing? The business risk associated with the transfer of personal information didn't result from the EKOS survey or customer concerns. The risks are a direct result of the increased visibility and concerns related to the USA Patriot Act in Canada. The Act provides US authorities unfettered access to any personal information held by US firms, whether it is on US citizens, Canadians, or anyone.

At first, the corporate concerns centred on compliance with privacy laws in Canada, mostly the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), Canada's federal private-sector privacy legislation. PIPEDA governs all cross-border transfers of customer personal information by corporate Canada. Corporate

# NYMITY

Canada was concerned that the USA Patriot Act conflicted with the PIPEDA and their business practices could be found non-compliant with privacy laws in Canada. The question asked was:

“Does transferring personal information to the US put our organization on the wrong side of privacy laws in Canada?”

The answer isn't that straightforward. The answer, in pseudo-legal terms is, “It Depends.” If you are subject to BC's privacy law, FOIPPA, then yes, your organization would be found non-compliant and potentially subject to large penalties. As for Canada's privacy law PIPEDA, it is unclear. Many experts believe there are exemption provisions in PIPEDA that would allow for disclosures to US law authorities.

Should corporate Canada be concerned? Yes, as the liabilities go beyond the impact of non-compliance with privacy laws in Canada. The liabilities could include loss of contracts and reputations could be damaged from the unwanted media attention.

How does an organization mitigate risk associated with transferring personal information to the US? Understand the risks, get legal advice, and as always, take direction from the regulators—the privacy commissioners in Canada.

## **Implementing Recommendations from the Privacy Commissioner of Canada**

The Office of the Privacy Commissioner of Canada is the regulatory body that provides oversight for PIPEDA, the law that governs all customer personal information transferred to the US by corporate Canada. In a paper from the federal privacy commissioner to a provincial privacy commissioner, the federal commissioner stated:

“At the very least, a company in Canada that outsources information processing in this way should notify its customers that the information may be available to the US government or its agencies under a lawful order made in that country.”

This was considered by many organizations as instructive guidance on complying with PIPEDA.

# NYMITY

One of Nymity's customers, a Canadian bank, implemented this recommendation and provided notice to their customers that their personal information will be transferred to the US, and thus subject to US law authorities. The notice stated:

*"I acknowledge that in the event that a Service Provider is located in the United States, my information may be processed and stored in the United States and that United States governments, courts or law enforcement or regulatory agencies may be able to obtain disclosure of my information through the laws of the United States...."*

*"I acknowledge and agree that the ... paragraphs above constitute prior written notice to me of, and my consent to the collection, use and disclosure of my personal information as described above...."*

Implementing the commissioner's recommendations, quite ironically, found the bank subject to customer complaints and a commissioner's investigation. The complaints gained media attention, in fact, so much attention, that the complaints became public knowledge, and became one of the rare cases where a company's name was associated with a complaint.

In October 2005, the commissioner's office published the finding related to the complaints, and it was no surprise that the bank that had followed the commissioner's recommendations was found to be compliant, and the complaints were therefore not well-founded. The finding stated:

*"The bank took the appropriate step of being transparent about its practices of using a US-based third-party service provider for processing and about the possible risk that customer personal information might be lawfully accessed by US authorities."*

So, at least from the commissioner's office perspective, the bank was compliant with PIPEDA and now corporate Canada has further instructions on how to be onside with PIPEDA when transferring personal information to the US. In fact, the commissioner's office stated that the bank didn't need to get consent, notice would have been sufficient, as the consent created the impression that a customer could opt-out of having their information transferred to the US.

# NYMITY

What does the commissioner recommend? Obviously, comply with PIPEDA, which states:

*“Principle 4.1.3 of Schedule 1 states that an organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Principle 4.8 provides that an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.”*

To comply, the finding states:

“What the Act does demand is that organizations be transparent about their personal information handling practices and protect customer personal information in the hands of foreign-based third-party service providers to the extent possible by contractual means.”

Simple enough, but will implementing these measures mitigate the risks associated with transferring customer information to the US? Possibly, from a compliance with PIPEDA standpoint. But does providing notice result in different business risks?

## **Business Risk Related to Providing Notice**

Now corporate Canada has new questions to ask:

“What are the risks associated with providing notice to our customers that we transfer their personal information to the US?”

“Do we really want to explain to Canadians, or to the media, that their personal information is accessible by US law authorities?”

“Do we inform Canadians if their information is breached in the US? What would be the impact?”

# NYMITY

“Will this disclosed business practice become a competitive tactic used by our Canadian-based competitors?”

“Will providing notice to consumers reduce consumer trust and have a negative impact on the brand, and on business?”

Is providing notice reducing business risk or increasing risk? Isn't it possible that some consumers could then look for an organization that isn't in the practices of transferring information to the US? If you, as a Canadian consumer, had to make a choice between two organizations, all other things being equal, wouldn't you choose the organization that maintained the data “out of harms way” of the US authorities?

Providing notice seems to at least create more questions, but what about business risk? Clearly, in the bank's case above, the unwanted media attention had a cost, including an impact on its reputation. In speaking with the bank, they indicated that doing the right thing is most important, and if they had to do the same thing over again, they would. But, have we seen other financial institutions providing notice? Actually, yes, but often in less “noticeable” ways, like changing the organization's privacy policy.

As providing notice could bring attention of this business practice to privacy advocacy groups, the media or even to your competitors, maybe it is better to take one's chances with exemptions within PIPEDA and forgo providing notice. For some organizations the answer is clear: provide notice. But for most organizations the answer isn't so straightforward, but in all cases one thing is clear, the organizations should assess their business risk associated with the transfers of personal information to the US.

## **About Nymity**

Nymity provides research, education and support services for privacy professionals tasked with providing privacy expertise to corporations and not-for-profit organizations with operations in the US and Canada. For more information visit [www.nymity.com](http://www.nymity.com).