PIPEDA and Online Backup

White Paper

The cloud computing era has seen a phenomenal growth of the data backup service industry. Backup service providers, by nature of their business, are compelled to collect valuable personal information about their subscribers, and it is critical that this information is kept private, secure and inaccessible to unauthorized individuals at all times.

Now this is also legally mandated by the **Privacy of Information Protection and Electronic Documents Act (PIPEDA)**. Service providers who fail to safeguard the personal information entrusted to them by their customers by not complying with the provisions of this act may find themselves facing liability claims and fines, along with the potential of a devastating loss of customer confidence.

Contents

Introduction

There is no doubt about it; the modern era of the internet has ushered in a permanent and universal need for constant electronic communication between individuals and businesses. For this reason, legislation has been passed in the European Union, the United States of America, Japan, Hong Kong, Dubai, Australia and New Zealand to make electronic commerce safer and more efficient, with an emphasis on protecting the individual's right to privacy and security of their personal information that they entrust to businesses. PIPEDA was introduced on the 1st of January, 2004 in Canada for this very reason, bringing Canada in alignment with the requirements of the European Union (EU), as well as many other nations around the world where privacy of personal information is mandated by law. In addition to this, PIPEDA was further strengthened by the amending of the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act, all of which served to help safeguard the transfer and usage of information between businesses and individuals in Canada.

PIPEDA Provisions

PIPEDA aims to create a legal framework concerning the individual's right to privacy of his or her personal information and the ways and means in which said information can be used by the data collecting entity for electronic commerce (or any kind of business, for that matter). The enactment of this legislation is “consent-based”, making it so that backup service providers who are collecting customer information must now clearly state the purpose for which the information in question is being collected, including letting the customer know what the information will be used for and the terms of disclosure. Indeed, obtaining explicit consent of the individual or enterprise entrusting the personal information is now a top priority. It follows that the information collected must be securely processed and remain inaccessible to unauthorized personnel, third parties and those who are not expressly permitted by the individual or enterprise to view the data.

The Rights of the Individual or Enterprise under PIPEDA

The individual or enterprise consenting to provide personal information to a backup service provider must know:

- Why the backup service provider is collecting personal information
- How the personal information collected will be used
- Who will have access to the personal information entrusted to the backup service provider
- How the personal information will be protected and secured by the backup service provider
- How the information will be destroyed when it is no longer required by the

backup service provider
- How the service provider will ensure that the information is accurate, up to date and complete at all times
- How the individual or enterprise will be able to access, update or request corrections to their personal information
- What remedy will be available to the individual or enterprise if the privacy rights are not respected by the backup service provider
- Whether they have the right to ask why they need to provide personal information, or the right to refuse to provide certain types of personal information, if the reasonableness of the request is not clear

Legal Compulsions under PIPEDA for Backup Service Providers

Unlike businesses that collect personal information for journalistic, artistic or literary purposes, backup service providers are subject to the provisions of PIPEDA, regardless of the size of the backup service provider in question or whether or not they operate exclusively online.

PIPEDA mandates that backup service providers must:

- Obtain the consent of their customers for all transactions involving the collection, use and disclosure of their personal information
- Provide backup services to their customers even if they refuse to give consent for the collection of personal information (unless, of course, the information in question is vital to the transaction)
- Collect the information by lawful means
- Formulate, implement and display prominently the personal information policies required of the backup service provider in order to encourage customer understanding of these policies

Exceptional Circumstances for the Disclosure of Information

In the event of an emergency, backup service providers reserve the right to disclose their client's personal information to the police, if indeed they are requested by them to do so, and proceed with such a disclosure without obtaining the consent of the information owner in question.

Where PIPEDA Does Not Apply

Enterprises within British Columbia, Alberta and Quebec are currently not covered by PIPEDA, but must still operate under similar provincial statutes. In those provinces,

PIPEDA still applies to organizations that are under federal jurisdiction.

Implementing PIPEDA

Implementing PIPEDA can bring about potential challenges to some backup service providers, with a number of operational difficulties often surfacing that will indeed have to be overcome. The act impacts technology processes, the elements of a business' reputation and the nature of governance itself. While implementing the provisions of this act, backup service providers will have to consider information technology risks, operational risks, human resources risks, finance strategies and customer relations. Any non-compliance with PIPEDA will bring about the potential of criminal prosecution, civil action and the possibility of damaging the reputation of the backup service provider in question.

In brief, PIPEDA demands that backup service providers comply with the following tenets while collecting, using or disclosing personal information:

Backup service providers must:

- Remain accountable
- Understand and implement processing limitations responsibly
- Ensure that the purpose of any exchange of personal information is specified and consented
- Ensure that the quality of information is optimized and updated by the information owner
- Ensure transparency and openness
- Implement security safeguards at all times to the best of their ability

The Impact of PIPEDA

No backup service provider wants to be perceived as being “behind the curve” in the implementation of PIPEDA. PIPEDA-aware backup service providers are continuously:

- Conducting privacy gap analysis to identify and control weaknesses
- Setting up remediation programs to address such control weaknesses
- Assessing cross-border data transfers to ensure adequate levels of protection
- Compiling and updating privacy policies and procedures to meet with compliance mandates
- Implementing employee and customer information protection awareness programs
- Auditing third party data processes for compliance to privacy agreements
- Updating third party contracts

Conclusion

PIPEDA is, above all, a human rights enactment and thus a celebration of the liberty and right to privacy of all people living in this increasingly digital age. It serves to draw attention to the risks involved in disclosing personal information without guarantee of security and demands new levels of customer consciousness concerning the risks he or she may be taking when consenting to share personal information with third parties without regard to consequences. Finally, it serves to hold backup service providers to new, higher standards of accountability, responsibility and security when it comes to how they handle the acquisition, storage and dissemination of their customers' valuable personal information.