

## **Small firms grapple with new privacy law**

Jan. 1 deadline looms: Companies 'ignore the act at their peril'

Paul Lima  
Financial Post

Monday, October 20, 2003

Effective Jan. 1, Ivon Hughes will not be able to run his business, Hughes Trustco Group, the way he has for the past 30 years -- without additional work. Currently, the Montreal-based insurance broker sends customers updates on existing policies and new programs. All that changes once Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) takes full effect.

Under PIPEDA, businesses can no longer collect, use or disclose personal information without consent. Federally regulated companies -- banks, insurers, telecommunications and transportation companies -- have been subject to the act since 2001. Effective Jan. 1, 2004, it covers all commercial activity.

Like many small and medium-sized business owners, Mr. Hughes, 60, is already chief cook and bottle washer. He will soon be CPO -- chief privacy officer.

PIPEDA dictates that every company must designate a priv-acy officer who is responsible for conducting personal inform-ation audits, ascertaining what personal information -- any data beyond what one might find on a business card is collected and determining how it is used, says Allan Macdonald, a Vancouver-based lawyer.

For example, newspapers and general interest magazines will no longer be able to sell names and home addresses of subscribers to third parties without the consent of subscribers. However, companies that sell goods or services to other businesses can still send customers marketing and promotional information. Sales representatives also can continue to send birthday cards or anniversary greetings to clients.

"The act is not meant to be interpreted in such a way as to be ludicrous. There is implied consent for innocuous situations that nobody has objected to," says Mark Hayes, a Toronto partner with the law firm Ogilvy Renault.

So, what do small to mid-sized enterprises have to do to comply?

First, they must determine if they have major privacy issues, says Jill McCutcheon, a lawyer at Blaney McMurtry LLP in Toronto. That takes work. "Don't miss the meeting about privacy or you will be the person put in charge," she jokes.

Even if businesses have the consent of consumers to send information, they must offer a "quick, easy and inexpensive" way to opt out or revoke consent, Ms. McCutcheon says.

PIPEDA also requires companies to safeguard private information, but it does not say how to do so.

Mr. Hughes, who supports an individual's right to privacy, does not know if password protection will suffice or if he has to encrypt data. He wants to market his products in a business-like manner and is concerned nobody has told him what he is supposed to do to comply with PIPEDA.

"I'm prepared to follow the guidelines once I know what they are," Mr. Hughes says. He does not think he should have to pay for lawyers or consultants to ensure he is compliant, and he says he believes the government has been less than forthcoming with information about the act.

Based on information from the federal privacy commission, many industry associations have established guidelines their members can follow, says Carolyn Burke, chief executive of Integrity Incorporated in Toronto.

The commission has put the full act on its Web site -- [www.privcom.gc.ca](http://www.privcom.gc.ca) -- including resource links for individuals and businesses.

Ms. Burke points out different businesses have different compliance needs: "It's kind of like Y2K. There is no one solution [that] fits all companies." Even so, "there will be significant overhead" for small businesses.

Overhead might include privacy consultants who will conduct privacy impact assessments, determine which policies companies need to change and produce privacy compliance road maps, she says.

There may be additional costs as privacy commission rulings, court decisions and case law have an effect on the nature of the legislation that is, admittedly, somewhat vague, says Robert Parker, a partner at Deloitte Touche in Toronto.

However, he says compliance should be viewed as an investment. "Privacy and trust are becoming business differentiators. Implementing and following a privacy policy is good for business."

Companies choose to "ignore [the act] at their peril," Ms. McCutcheon says. Consumers and privacy advocates may go public with complaints before giving companies the opportunity to rectify situations. This can lead to negative publicity, she says.

Businesses should look at the act as an opportunity to gain consumer trust rather than as something "to fear," she says.

Consumers have become more aware of privacy issues due, in part, to the proliferation of electronic databases that store personal information. It is ironic that at least one major technology company, IBM, offers a technology solution to privacy concerns.

IBM's Tivoli Privacy Manager allows organizations to manage consent and privacy preferences and provides reports on how data is used, says Tarun Khandelwal, an IBM software manager. It even enforces privacy policies, he says. If a sales representative tries to send marketing material to a consumer who entered an online

contest but did not consent to receiving promotional material, the software will deny access to the contact information on the company database.

Provinces can invoke their own privacy acts, which may differ from PIPEDA, compounding compliancy, Mr. Macdonald says. Quebec has a privacy act and Alberta and British Columbia will have acts by the end of the year. However, unless a provincial act is approved by the federal cabinet, PIPEDA takes precedence.

[fpedge@nationalpost.com](mailto:fpedge@nationalpost.com)

© Copyright 2003 National Post