

A LITTLE BIT OF INFORMATION FOR OUR FILES

by Craig A. Zawada

© 2002 Wallace Meschishnick Clackson Zawada

Psst. Come in a little closer. Let's share some secrets just between us. Ever enter some fake information on an Internet form? Maybe you fibbed about your annual income? Perhaps the name and e-mail address are all wrong?

You are not alone. Countless numbers of people are doing this, in part to object to the unrelenting collection of personal information in today's society.

The Net is not the only culprit here. We are inundated with forms at an ever-increasing rate. Want to rent a video? Fill out this form, please. Need a loan? Let me just get some information from you. Buying some software on the Net? Can you . . . well, you get the idea.

With all of our personal information open to scrutiny and sale, its no wonder that people are objecting to forms. I'm not recommending giving false information – it can be illegal in some cases. Still, why in the world would you want to disclose your hobbies to your computer manufacturer, without knowing how that information will be used?

The never ending supply of forms leads people to consider the protections granted to personal information. In short, there are hardly any. Data collectors are, for the most part, pretty much free to use information for whatever purpose they want. This may change, though, since Canada has moved (tentatively) into protecting personal information through *The Personal Information Protection and Electronic Documents Act*.

As its unwieldy name implies, part of the Act deals with using electronic documents and signatures in commerce, and this gathered most of the attention when the Act was passed in Spring, 2000. The privacy provisions are just as important, however, and are now in force for many organizations across the country.

The Act regulates the collection, use and disclosure of "personal information". Almost anything about an identifiable individual can be personal information, all the way from a home phone number to credit card information.

Nearly every organization (which includes businesses, corporations and individuals) must adopt a privacy policy to deal with personal information gathered and used by them. This framework is built around 10 principles, based on a model Code developed by the Canadian Standards Association in the mid-1990's. The principles are:

Accountability: A person or persons must be designated by the organization to implement and administer the policy.

Identify Purposes: The purposes for which information will be used and disclosed must be identified at or before collection.

Consent: Individuals must give their informed consent to the stated purposes.

Limited Collection: The data collected must be limited to the identified purposes.

Limited Use/Disclosure: The use and disclosure of information cannot extend beyond the stated purposes.

Accuracy: Data must be accurate and complete.

Safeguards: Information must be protected appropriately.

Openness: Information on the organization's policies must be readily available.

Individual Access: Individuals must be allowed to obtain information on their data and its use.

Challenging Compliance: The organization's compliance with these principles can be challenged.

There are some exceptions to the rules, but the majority of data collection activities in Canada will be covered. Even businesses that don't consider themselves to be in the "data business" need to comply. If your business simply takes down customers' addresses and phone numbers, that is considered to be personal information. Likewise, sending out Christmas cards to clients is a "use" of personal information.

The Act clearly encourages parties to work out disputes themselves. If they cannot, the federal Privacy Commissioner can investigate and make recommendations. Only in rare circumstances will the courts get involved.

While the lack of solid remedies may imply that this Act is optional, there are some significant consequences for non-compliance. The Privacy Commissioner can audit organizations' practices, and make public their policies. Privacy is such a hot issue these days that the threat of publicity will likely bring most businesses into line.

The Act applies, since January 1, 2001, to federal undertakings, and to transfers of personal information across provincial borders. A federal undertaking is most anything under national jurisdiction, such as grain companies, broadcasters, airlines, railways, and banks.

Personal health information has been covered since January 1, 2002. All other organizations will be brought under the Act's authority on January 1, 2004. If a province enacts similar legislation by that time, the provincial law will apply.

Those businesses that are not yet subject to the Act should not relax. For one thing, they may deal with federal undertakings, and may be contractually bound to have similar guidelines. More importantly, there is no grandfathering under the Act. Any data collected before January 1, 2001 is still covered by the Act. Compliance might as well start now, and it might even provide a market advantage to do so before competitors react.

So what should a business do? First, a privacy policy needs to be created in line with the Act's requirements. Not only must people be designated to be accountable for the policy, but everyone in the business should be aware of the responsibilities. Yes, this will mean extra work and record keeping. Consider the loss of goodwill, however, if customers feel you are unconcerned about their information.

This article is for general information only and relates only to Saskatchewan law. Specific situations may require different or additional information. Do not act on any information contained in this article without consulting your advisors regarding your specific circumstances. As well, some of the articles are of historical interest only because legislation or case law may have changed.