



Bailey Jung



# The Information Age:

## Protecting Your Financial and Personal Privacy

**A**s of January 1, 2004, all businesses in Canada that collect, use, and disclose personal information must comply with either:

- the *PIPED Act*, or
- a substantially similar provincial law.

The *PIPED Act* (*Personal Information Protection and Electronic Documents Act*) is new legislation implemented by the federal government to protect the privacy of Canadians in the private sector. The *PIPED Act* sets out the ground rules for how private sector organizations may collect, use, and disclose personal information, whether in the “real” world or on the Internet.

*PIPED Act*:

[http://www.privcom.gc.ca/legislation/02\\_06\\_01\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_01_e.asp)

[http://www.nymity.com/bc\\_pipa/](http://www.nymity.com/bc_pipa/)

While the *PIPED Act* is a step in the right direction and good news for Canadians, the public still needs to be vigilant and careful about the collection, use, and disclosure of information about them that is taking place without their knowledge or consent.

Note: In British Columbia, the *Personal Information Protection Act (PIPA)*, which essentially mirrors the federal *PIPED Act*, came into force January 1, 2004. It is our province’s response to the “substantially similar” privacy legislation requirement.

To view the *PIPA Act*, visit:

[http://www.qp.gov.bc.ca/statreg/stat/P/03063\\_01.htm](http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm).

Most people are aware of the Internet’s benefits and the role it has played in making our lives more convenient. Not everyone is aware of how the digital revolution and the Internet can threaten personal privacy, however. The past decade has witnessed the dramatic growth in the use of the Internet, to the point that it has become a true mass medium.

Ten years ago when I was still working for a national building supplies home improvement retailer, pricing information on every item we sold was stored on microfiche. We didn’t have the luxury of clicking a mouse to find out the cost of an item or if it was in stock.

That was only 10 years ago. Today, most businesses cannot fathom running a business without computers and all the benefits and conveniences the Internet provides. All this convenience comes with a price, though, and gives rise to a whole new set of political, social, and economic issues.

**Every day, businesses, organizations, and government agencies at all levels collect vast amounts of personal information about you and store the information in their databases.**

The enormous amount of information out there in cyberspace about you means that the possibility for infringing on your privacy and abusing the use of personal information about you is greater than ever before.

Every day, businesses, organizations, and government agencies at all levels collect vast amounts of personal information about you and store the information in their databases. The list is extensive; it includes your employer, credit bureaus, banks, brokerage firms, insurance companies, Land Title Office, motor vehicle branch, telephone company, utility company, crown corporations such as ICBC, provincial ministry of health, credit cards, department of vital statistics, Elections Canada, Human Resources Development Canada, BC Assessment Authority, Canada Customs Agency, and direct marketers.

The information that some of these organizations and agencies keep about you can be the most sensitive and personal information imaginable.

Many businesses can now track your buying habits, where you shop, the type of videos you like to rent, magazines to which you subscribe, where you like to travel—even the type of breakfast cereal you eat each morning. On the Internet, advances in technology and sophisticated software allow your every move online to be monitored. This means that when you go online, you leave an electronic fingerprint of your movements and, as a result, you can unwittingly provide personal information to people and organizations that track such data.

With a few clicks of a mouse, it is relatively easy for a complete stranger—who has access to a computer and a connection to the Internet—to compile a detailed profile of your personal and financial life.

I recently experienced firsthand the power of the Internet and the ease with which information can be obtained. I wanted to find out the birth date of a friend so I could surprise him. By performing a search using a combination

of his full name, occupation, and employer, I managed to secure the information I was seeking in less than 10 minutes.

Given the enormous amount of sensitive and personal information about you that is sitting in databases, as well as the frequent movement of such information, the potential for the misuse or abuse of such information could become a real nightmare if it falls into the wrong hands.

Although there is no single, easy solution to combat privacy and security abuse—and a person could write an entire book on the subject—consumers can take steps to minimize the chance of personal and sensitive information being used without their consent or knowledge.

**Many businesses can now track your buying habits, where you shop, the type of videos you like to rent, magazines to which you subscribe, where you like to travel—even the type of breakfast cereal you eat each morning.**

The following are a number of key tips to keep in mind the next time you are using the Internet and are asked to provide any kind of personal information.

- Refuse some or all of the “Cookies” that Websites send you. Cookies are small text files that Websites put on your hard drive. They can collect and store information such as the Internet Protocol (IP) address of your computer, the operating system you are using, banner ads you’ve clicked on, Websites you’ve visited, and any information—such as your name—that you may have voluntarily provided. Cookies allow Websites to quickly identify you as a previous visitor. This makes it unnecessary for you to go through the process of
- identifying yourself every time you visit a Website.
- Be careful about providing information, particularly information such as your date of birth, social insurance number, driver’s licence number, and credit card numbers. Even though many sites are supposedly secure, reports of professional hackers gaining access to databases containing confidential personal information suggests that no site is 100 percent secure.
- If you must provide personal information, provide only what is required and no more. For example, if you are purchasing a book online, there is absolutely no reason why you should be required to provide any more information than a name, shipping address, and a credit card number.
- Before you purchase anything online or conduct any kind of financial transaction, make sure you read and understand the Website’s privacy policy. If it doesn’t have one, you should think twice about making the transaction.
- Obtain a separate credit card with a low credit limit to use for all transactions you conduct online. By using only one credit card, you can keep a closer watch on any unauthorized charges on your credit card statements.
- Avoid using passwords that include information such as your name, mother’s maiden name, or birth date. Instead, choose a mixture of numbers and both upper and lower case letters. Changing your password periodically is also a good practice.
- Think of email as postcards others can read and even pass on to someone else. Sending confidential or sensitive information such as account numbers, social insurance numbers, and passwords should be avoided. If you must communicate privately or need

to send confidential information, install software that allows you to “encrypt” or scramble your email messages so that nobody can easily understand them but you and the person receiving your message.

### **Conclusion**

The Internet and the digital economy are here to stay. While advances in technology have been widely heralded as making our daily lives more enjoyable and convenient, it has also created a new set of issues and challenges. The collection and use of personal and financial information by unscrupulous individuals and businesses to commit fraud and identity theft is a serious problem; every consumer must take some measure of responsibility for combating it.

Consumers must become more assertive in demanding that their personal information be protected and that they be given greater control over the collection and use of such information. ▲

**For instructions on how to delete Cookies, please see Techno Tips article on page 25.**

*RBC Dominion Securities Inc. is a member company under RBC Investments. RBC Dominion Securities Inc.\* and Royal Bank of Canada are separate corporate entities, which are affiliated.*

*\*Member of CIPF*

*The views and opinions of this article are those of the author and not necessarily those of RBC Dominion Securities Inc. Any opinion or advice contained in this article should not be construed as offering professional advice. Readers are advised to consult their own professional advisors regarding their own situation.*

**Bailey Jung** is an Investment Advisor with RBC Dominion Securities Inc. in Vancouver. He provides wealth management solutions and financial planning services to his clients.

Voice: 604 665-0673  
bailey.jung@rbc.com  
www.rbcinvestments.com/bailey.jung