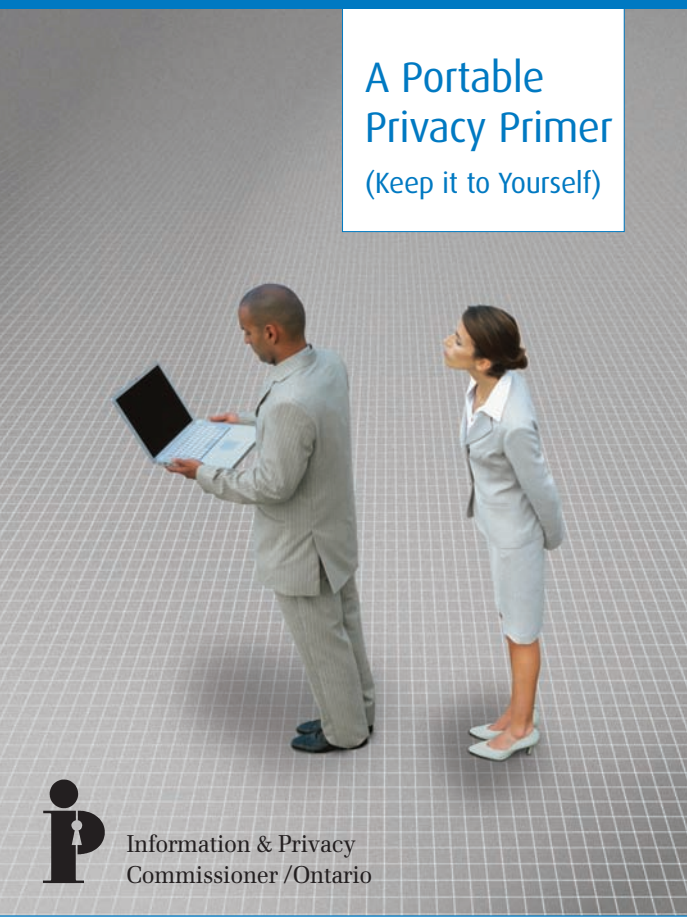
Reduce Your Roaming Risks

A Portable Privacy Primer

(Keep it to Yourself)



Information & Privacy Commissioner /Ontario

BMO Financial Group

Today, you have the flexibility to connect to your organization's network from virtually anywhere in the world.

Working away from the "bricks and mortar" office means that you are also working outside the traditional security layers. As a result, you need to re-assess the privacy and security risks associated with working remotely or while travelling. You need to take appropriate steps to safeguard confidential information, whether it's your own information, that of your employer, or, most importantly, that of your clients.

In this brochure, we look at some of the risks associated with "mobile" technology (especially while away from the traditional office) and offer advice on how to reduce these risks. This advice may assist business travellers, home care providers, professionals offering on-site consulting, freelancers, or simply employees taking their work home or on the road.

1 Identity Theft

Identity theft (ID Theft) is the theft of one's personally identifiable information and the use of that information with the intent of committing fraud or other crimes in the victim's name.

It can happen even more easily when you are in transit. Here are some of the typical ways for identity thieves to acquire information:

1. **Theft of equipment** – laptops, Personal Digital Assistants (PDAs) or cell phones – from cars, public transit, hotel rooms, public places, airports, etc. If the equipment has unencrypted personal information on it, your clients may be at risk of ID theft and your employer may be at risk of negative publicity and media attention, lawsuits and other legal sanctions.
2. **Dumpster diving** – in trash bins in your hotel room or wherever you throw away your personal information, such as credit card statements or purchase receipts.
3. **Shoulder surfing** – when using your debit or credit card, at an ATM or when you work on your laptop or PDA in public places.
4. **Spyware** – which is easily installed when you connect your unprotected laptop or PDA to a public network.
5. **Phishing** – e-mails which may trick you into divulging personal information.

2 Develop a Privacy and Security Mindset

There are people who will try to steal, damage or misuse important personal or business data that is in your possession – either in paper or digital format. Don't become a target! Learn how to protect yourself and your organization.

3 Protect Your Clients, Your Organization, Yourself

To protect your clients, your organization and yourself, we recommend the following:

1. Do not remove any client information from your organization's network without authorization from your supervisor and without, at the very least, strong password protection, and preferably, data encryption.
2. Only conduct confidential business on business or personal computers. Do not use public computers or networks, or conduct business in public places.
3. Do not discuss confidential information on your cell phone in public places.
4. Remove confidential information, or any devices containing confidential information, from plain sight in your vehicle. Lock your valuables in the trunk **before** you start the trip, not in the parking lot of your destination.
5. Remember to collect all of your belongings when you leave: a cab, hotel room, meeting place, airplane, or restaurant.
6. Leave unnecessary identification (such as SIN card, birth certificate, health card, etc.) at home unless you really need to carry them. Store them in a hotel safe while travelling.
7. Put all receipts in your wallet, not in shopping bags, and do not leave receipts in hotel rooms or vehicles.
8. Retain your hotel room magnetic key, boarding passes, anything that may have your personal information on it, until you can shred it or destroy it securely.

9. Always review your bank and credit card statements for any unusual activity as soon as you receive the statements.

Key Principles:

1. **Minimize** the amount of personal or business data you carry with you – make sure that you actually need all the data.
2. Do not remove any personal or business data from the office without **authorization**.
3. Employ all physical and technical means to secure the data you carry with you. **At the very least, use a strong password to protect the data. For even stronger protection, you should use encryption.**

4 Laptops, PDAs, Cell Phones

Laptops, PDAs and, more recently, cell phones are considered to be the "golden eggs" by information thieves. Take the following precautions to minimize the risks:

1. Ensure that all of your devices require passwords for access: power-on passwords, screensaver passwords, account passwords.
2. Strong passwords consist of at least eight characters, upper and lower case, numerals and special characters. The password should not be a word that can be found in any dictionary.
3. Protect your passwords and encryption keys by NOT writing them down.

   Note: there are innovative programs for PDAs (signature-based, or tapping a certain point on a picture) as alternatives to having to retype your password.

4. Enable the automatic lock feature of your device after five minutes of idle time.
5. Avoid carrying confidential data on your mobile device unless you absolutely must.
6. Encrypt your data according to your company's approved policies. This is essential if you transport personal and/or confidential customer data – it should never be left in "plain view".
7. When no longer needed, remove all confidential data from your devices using a strong "digital wipe" utility program. Do not rely on the "delete" function to remove confidential data.
8. Use a lockable briefcase or laptop case that does not bear any visible logos of high-profile companies or associations.
9. Place an "if found, return by calling [phone number]" card inside your briefcase, with no other identifying information.
10. Secure your mobile devices at all times. Use a cable lock with an audible alarm when working on them, or lock them away when not in use.

When using mobile devices featuring Bluetooth technology, you will be more secure if you:

1. Turn off Bluetooth when not needed.
2. Keep devices set to "non-discoverable."
3. Use as many characters as possible for your Bluetooth PIN.
4. Configure these settings in a private location.

5 Confidential and Financial Information

If you handle confidential information online or perform financial transactions, then your laptop (and sometimes your PDA) should, at a minimum, have personal firewall, anti-virus and anti-spyware protection. Follow the **I-C-U** cycle: **Install** soon, **Configure** properly, **Update** regularly.

In addition, make sure you have installed the latest updates and security patches for your mobile devices, including your cell phone.

When connecting to public wireless networks or HotSpots in airports, hotels, coffee shops, public libraries, etc., bear in mind that these networks are inherently unsafe. Remember the following:

1. Watch out for shoulder surfing – someone "casually" observing the work on your laptop.
2. Never connect to two separate networks simultaneously (such as Wi-Fi and Bluetooth).
3. Do not conduct confidential business unless you use an encrypted link to the host network (such as a Virtual Private Network – VPN).

Unless encrypted, all the information on the Internet travels in plain view, accessible to anyone. This premise applies to web browsing, e-mail and Instant Messaging.

Key Principle:

If you don't know how to use the technical safeguards in this brochure, and cannot implement them yourself, ensure they are done on your behalf, before you take any personal information away from the office.

6 If You Become a Victim of ID Theft

The most important thing to do is to act quickly and assertively to minimize any possible damage.

1. Begin by documenting all the conversations you have including dates and times, names and phone numbers, when dealing with the authorities and financial institutions.
2. Immediately report the crime to law enforcement departments – police (and possibly PhoneBusters) and file an occurrence report.
3. Armed with your occurrence report, contact the credit bureaus listed below in the **contact information** section and ask that your file be flagged with a **fraud alert**.
4. Contact all creditors with whom your name has been used fraudulently, by phone and in writing.
5. Tell any debt collectors who subsequently call you that you are a victim of identity theft and are not responsible for unpaid bills on fraudulent accounts. Be sure to obtain the pertinent information about these accounts to complete your report to the authorities.
6. Report the loss or theft of your passport immediately to both local police and the closest passport office (www.ppt.gc.ca/can/lost_stolen.aspx?lang=e). If you are outside Canada, report it to the nearest Canadian Consulate or Embassy.

Key Principle:

If you lose confidential data, especially client personal information, notify your supervisor and privacy officer in your organization immediately.

QUICK REFERENCE CHECKLIST

Before you take anyone's personal and confidential information out of the office, check this list:

1. Do you have permission from your supervisor and/or organizational policy?
2. Are you taking as little personal information as possible and, preferably, no Social Insurance Numbers?
3. If electronic information is being taken,
   a. Is it password-protected?
   b. Is it encrypted?
4. Is your briefcase or laptop case locked and unmarked?
5. Do you know what to do in the event of a theft or loss of data?

ALWAYS REMEMBER:

Lock it, password it, protect it.

Contact information

Credit Bureaus

Equifax	1-800-465-7166 www.equifax.ca
TransUnion	1-866-525-0262
Quebec residents	1 877 713-3393 www.tuc.ca
PhoneBusters	1-888-495-8501 www.phonebusters.com

Identity Theft

RCMP
www.rcmp.ca/scams/identity_theft_e.htm

Government of Ontario
www.cbs.gov.on.ca/mcbs/english/ID_theft.htm

BMO Financial Group
bmo.com

Information & Privacy
Commissioner/Ontario
www.ipc.on.ca
Ann Cavoukian, Ph.D.
Commissioner
August 2006

Privacy-IPC (08/06)

BMO Financial Group