Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Fact Sheet

Number 14
August 2007

Wireless Communication: Safeguarding Privacy & Security

We are fast approaching the point where it is reasonable to assume that any device that creates or stores data either has, or is connected to, some form of embedded wireless capability. Cell phones and personal digital assistants (PDAs) are increasingly sophisticated, often combining multiple wireless technologies in a single device.

Wireless technologies can reduce costs, increase efficiencies, and make important information more readily and widely available. In the health care sector, for example, wireless data communications now make it possible for paramedics to send cardiac images and data directly to cardiologists, significantly reducing wait time to treatment.

Clearly, the benefits of wireless communications are many. But, there are also risks. Without appropriate safeguards, transmitting data wirelessly can be like using an open filing cabinet in a waiting room. In fact, this Office just recently issued an Order about a case where unauthorized viewers had inadvertently intercepted wireless video images of patients in a washroom providing urine samples.

This Fact Sheet addresses privacy issues arising from the use of wireless technologies, expanding on Fact Sheet #13, *Wireless Communication Technologies: Video Surveillance Systems*.

Taking Care

The *Personal Health Information Protection Act* (PHIPA), the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) set out requirements for the protection of personal information, including information in electronic form.

In general, compliance with these *Acts* requires that those responsible take reasonable measures to protect personal information, which may include physical safeguards, using role-based access to personal information, or technological measures such as encryption.

The transmission of personal information in electronic form, particularly through the use of wireless technologies, means adding "data-in-motion" to "data-at-rest" as a category of data to protect, and adds another layer of complexity to compliance with these *Acts*.

A good starting point for understanding the impact of technological change or new developments is to regularly re-examine past assumptions and decisions. A reasonable precaution is one that any prudent and privacy conscious individual or institution would take. For example, there was a time when it was reasonable to browse the web and download files without

a personal firewall or anti-virus software. This is no longer the case today.

Those responsible for the acquisition, implementation or use of electronic devices that contain or have access to personal information must proactively take steps to protect that information. This may require specialized technical knowledge. If those who are responsible do not have such expertise, they should seek the advice of experts.

Wireless Communication Technologies

Wireless devices have a number of common characteristics. The most significant is that they broadcast information over radio waves.[1] Though they may be encoded differently (some analog, some digital), all radio waves are broadcast in all directions from the point of transmission.

This means that any receiver within range that is tuned into the frequency of the signal will receive it. Systems administrators are not able to identify who has accessed the signal, which means that inadvertent disclosure to unauthorized parties is easily possible.

Any time wireless technology is used to transmit personal information, that information must be strongly protected to guard against unauthorized access to the contents of the signal.

Sometimes, the mere existence of the signal can divulge personal information. This is the case, for example, with cell phone or other mobile transmissions that reveal a person's location and movement patterns.

Wi-Fi

Wireless Fidelity (Wi-Fi) refers to a range of technologies for wireless data networking (See Table 1 below).

Wireless data networking links computers without wires. Because of its low cost, a wide range of individuals, many of whom are not networking specialists, now use Wi-Fi equipment. Wireless routers, for example, are increasingly common in home or small office computer networks.

If the data are not encrypted, however, or if an outdated and inadequate form of encryption is used (e.g., Wired Equivalent Privacy or WEP), personal information transmitted over these wireless networks is vulnerable to interception. It is believed that a WEP-encrypted wireless network allowed thieves to steal the credit and debit card information of over 45 million T.J.Maxx customers.

Use up-to-date transmission encryption to minimize the risk of unauthorized interception. Large organizations may wish to use virtual private networks (VPNs) for mobile workers, while individuals or smaller organizations may use Wi-Fi Protected Access (WPA or WPA2).[2]

Remember that any wireless-equipped device connected to a network can serve as an illicit entry point for the entire network if it is not properly set up. Breaches that involve information systems can run the risk of disclosing entire databases of personal data. To prevent data leakage from wireless access points it is vital to secure the entire network, rather than only specific devices.

1 Strictly speaking, infrared devices are also wireless, but because of their limited and decreasing use, they are excluded from this fact sheet.

2 WPA and WPA2 are generally regarded as secure, as of the time of writing of this fact sheet. Remember that standards change quickly and to check this with your service provider.

Bluetooth®

Bluetooth® technology connects electronic devices using short-range wireless signals. It is used to link cell phones to headsets, keyboards to mice, and laptops to printers through a "pairing" process.

Though security options are available, some of these systems are not fully secure. Unauthorized access through *bluesnarfing*, *bluejacking*, and *bluebugging* are well documented.[3] Of these, the most serious is bluesnarfing, which allows unauthorized access to data stored on a vulnerable Bluetooth® device.

Not all devices are equally vulnerable, and manufacturers are currently making efforts to address security issues. Nonetheless, ensure that all your Bluetooth® devices are appropriately secured, and that any personal information transmitted is de-identified.

Do not enable Bluetooth® on any device containing or having access to personal information without confirming that the connection is in fact secure and protected.

Transmitters on Chips

Wireless technology can be embedded in or attached to a chip. This is the case with Radio Frequency Identification (RFID) chips.[4]

RFID chips have many applications. In the health care sector, for example, there are now systems where RFID tags are used to match patients with their prescription, preventing medication or dosage errors.

Other similar technologies include contactless smart cards and Near Field Communications (NFC) devices. Contactless smart cards are in use as credit and debit cards, while NFC-enabled cell phones are being used for micro payments to vending machines. The increased use of transmitting devices for the purpose of conveying financial information, if done without sufficient attention to security, can expose users to identity theft and other threats to their privacy.

Where embedded chip devices collect or use personal information, ensure that encryption or similar strong security measures are in place. The information systems to which the devices are connected should provide "end-to-end" security for personal information.

Cellular phones and PDAs

Cellular phones and PDAs are rapidly converging and may be regarded as a single category. They can be used not only for voice transmission, but also as wireless modems or web browsers. When used to transmit or store email or instant messages, these devices can pose risks.

Make sure that you set up cell phones and PDAs to operate in a secure manner. Security features include the encryption of transmissions, password protection, and automated data wiping.

It is also important not to use cell phones or PDAs to discuss personal or sensitive business information in public places.

When using data features on cellular phones, PDAs, or similar devices, do not let their small size deceive you into treating the data with less care than you would on your desktop computer or laptop.

---

3 For example, see Carettoni et al, "Studying Bluetooth Malware Propagation: The BlueBag Project" *IEEE Security & Privacy*, March/April 2007, Vol. 5, No. 2, pp 17-25.

4 *Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)*: **http://www.ipc.on.ca/images/Resources/up-1rfidgdlines.pdf**

Conclusion

The use of wireless devices is here to stay. The number of devices, and more importantly, the types of devices, will only increase over time. There are undeniable cost benefits and increases in efficiency that can be derived from their use. But these benefits will only be actualized if a culture of privacy is developed. As wireless communication technology becomes fully integrated into information systems and business processes, it is inevitable that substantial amounts of personally identifiable information will flow over the airwaves. Since radio waves are a broadcast medium, capable of being received by anyone who is in range, reception of the signal by unauthorized receivers cannot be prevented. Therefore, those responsible for personal information must ensure that "data-in-motion" must be strongly encrypted at all times.

Table 1 Categories of Wireless Networks[5]

	Personal Area Network (PAN)	Local Area Network (LAN)	Metropolitan Area Network (MAN)	Wide Area Network (WAN)
Technology	Bluetooth Ultra-wideband (UWB)	802.1b 802.1a 802.1g a.k.a. Wi-Fi	802.16 802.16a 802.16e a.k.a. WiMAX	GSM GPRS CDMA 2.5G 3.5G
Data rates	Medium data rates 1Mbps to 2Mbps	High data rates 11Mbps to 54Mbps	Very high data rates Quality of Service up to 268Mbps	Low to medium rates 10Kbps to 2.4Mbps
Range	Very short range 3m (~10 feet)	Short range 100m (~300 feet)	Medium range 50km (~31 miles)	Long range Global
Connectivity	Notebook to PC to peripherals Devices to systems	Computer to computer and the Internet	LAN or computer to high-speed wire line Internet	Smart phones and PDAs to WANs and the Internet

5 Table in Dekleva, Sasha et al. "Evolution and Emerging Issues in Mobile Wireless Networks" *Communications of the ACM*, June 2007, (Vol. 50, No. 6), p. 41.

Fact Sheet

is published by the **Office of the Information and Privacy Commissioner/Ontario**.

If you have any comments regarding this newsletter, wish to advise of a change of address, or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Cette publication, intitulée « Feuille-info », est également disponible en français.

30% recycled paper