THE GLOBE AND MAIL
Published in the *Globe and Mail* 19 August 2006

Keeping private talk private

As the Royal Family has discovered, your phone, BlackBerry and computer are all vulnerable to hacking. DAWN RAE DOWNTON explains what you can do about it .

DAWN RAE DOWNTON

HALIFAX -- Just how easy is it to hack a cellphone?

Last week, Britain's Prince William seemed a victim of high-tech eavesdropping when details of private meetings he had arranged by phone showed up in the London tabloid News of the World. Over breakfast, Britons read about gear the Prince had borrowed from a friend, even the particulars of an appointment he had made with a surgeon about his bad knee. But it turns out it was his voice mail, not his phone, that was "tapped."

In the United Kingdom, cellphone signals can be intercepted, but they are hard to decode. In North America, slacker telephone technical standards make hacking a little easier.

Prince William, who poses for a cellphone picture with Dylan Harris in Auckland last month, was recently a victim of voice-mail hacking.

Not only celebrities need worry. Employers and employers-to-be, competitors, convicts, garden-variety enemies, nosy friends, suspicious spouses and disgruntled exes, all these can bring unwanted attention to ordinary you.

It's not only your cell that's vulnerable. There's your land line, your cordless, your BlackBerry and your e-mail. What's most at risk? How can you protect yourself?

Cellphones

Police, intelligence agencies, private business — any of these can listen in on your digital cell if they want to. All it takes is a half-million-dollar scanner that is illegal in North America, except to intelligence interests and law-enforcement agencies. Cell scanners are readily available and mostly legal elsewhere in the world, but they are not cheap anywhere. In Canada and the United States, governments and security agencies have them. Pinkerton's and the like probably have them too. Your neighbour most likely does not.

With 75 per cent of the market, GSM (Global System for Mobile Communications) is the cell technology used most worldwide. CDMA (Code Division Multiple Access) is the runner-up. Because both systems are digital, they are widely regarded as secure, but they are not. Scanners break them in Canada and the United States because transmissions are only loosely encrypted here. Researchers at the University of California at Berkeley cracked a European conversation in less than two minutes, while a North American call took less than a second to break.

GSM data are “protected” by 64-bit encryption — 64 bits of data are used in the keys that encode and decode transmissions. But the Berkeley team found that the GSM code here (and in other European export markets) is purposely downgraded from the 64-bit standard to only about 40 bits. On this side of the Atlantic, the dedicated hacker has a simpler cipher to break.

Why the difference, continent to continent? Industry sources say U.S. intelligence agencies want to be able to monitor cells with little effort.

Originally, cell technology was not digital but analogue, transmitting audio in its original form, undigitized. For instance, the voices you hear on the radio are analogue.

Analogue phones are still used throughout the world, even in North America, and monitoring an analogue call with a hundred-dollar scanner from Radio Shack is a walk in the park.

How to protect your digital cell? A $2,000 scrambler from any number of on-line vendors will help, but perhaps only a bit since the air portion of your transmission may not be encrypted by your phone company and your scrambler can't compensate. But it will work gangbusters in protecting your analogue phone.

So how do governments secure their cell calls? Ottawa and Washington use the Sectera Timeport 280 GSM, a basic Motorola phone that has been beefed up by a military contractor, General Dynamics. Sectera use is heavily restricted, and its export prohibited, except to “friendly” countries. Replacing the STU-III secure telephone that used to grace the ambassador's desk at U.S. embassies worldwide, it can access GSM networks in at least 200 countries.

With 256-bit encryption, Sectera isn't going to be hacked any time soon. The good news for consumers? General Dynamics is working on a commercial version, and for $2,500 (U.S.), it is already selling a reduced-encryption model called TalkSecure.

Land lines

Your telephone is wide open to government and intelligence-agency eavesdropping, as is your Internet use and your e-mail (see below). Anyone else will have difficulty tapping your phone, though it used to be easier a few years ago when analogue ruled. A casual eavesdropper can still break into your house and tap the junction box in your basement — or simply bug the desk lamp beside your phone.

For protection (except from the lamp bug), you can use a scrambler on your land line.

Cordless phones

Don't discuss sensitive matters on your cordless. It has no protection against eavesdropping and can be picked up as far away as 500 feet. The “spread spectrum” technology in many newer cordless phones makes them less susceptible to monitoring but by no means secure.

Last month, a retired man in Halifax outraged his neighbours by announcing that for fun he had intercepted a month's worth of their cordless chat on a police scanner. He was reported to Industry Canada.

BlackBerrys

If you think your BlackBerry is bulletproof, you're wrong.

Just two weeks ago, a whiz at the Las Vegas DefCon 14 hackers conference flaunted a malicious piece of software called BBProxy that can burrow its way into the BlackBerry network.

Time will tell whether BBProxy spawns imitators, which would force Research in Motion, BlackBerry's maker, to circle its wagons the way virus developers did Microsoft.

Protection? RIM says that if users configure their BlackBerrys according the manual, there is no problem.

Wireless Internet

See for yourself how easily it's hacked: Drive down a city block with your WiFi laptop and watch every WiFi system in the houses you pass pop up on your screen. Protect your system with encryption.

Internet, e-mail, VoIP

Your Internet activity is watched relentlessly by marketers using spyware to know where you go and what you look at.

Hackers — not the rascals who want to wipe your hard drive clean, but the predators — cruise the net looking for credit-card numbers and other tidbits useful in identity thefts.

Use a firewall and anti-virus and anti-spyware software against these Internet snoops.

Other kinds of data miners ask for your particulars openly. Just last week, for instance, Amazon filed a patent to gather information voluntarily from its 59 million shoppers about their religion, sexual orientation, ethnicity and income. The company says it has no immediate plan to act on its patent.

That's the commercial picture. Given the number of methods by which you can be hacked, it's the stuff of legend. So is the degree to which your e-mail and browsing habits are monitored by government.

The capability has existed for years, since telephone and Internet switching follows “intercept compatible” specifications set down globally by the International Telecommunications Union and enshrined in CALEA, the U.S. Communications Assistance for Law Enforcement Act.

ENFOPOL 98 imposes similar specifications on telecommunications in Europe.

The Canadian counterpart, the Modernization of Investigative Techniques Act (Bill C-74), died with the last government. Experts think it may reappear before Parliament this fall.

CALEA, developed 15 years ago by the U.S. Federal Bureau of Investigation with the assistance of Canada's Nortel Networks, lets its investigators tap into any communications channel in the world from the comfort of home. Any land-line call can be heard, any e-mail or instant message read, any Web travel tracked.

Voice over Internet Protocol, or VoIP, is a new way of talking long distance over the Internet that looked like it might escape CALEA, but that loophole has been closed. If you talk through Vonage, Big Brother may be listening.

Both Canada and the United States prohibit their security agencies from eavesdropping on their own citizens, though a half-century-old treaty between our countries allows each to snoop domestically for the other. The protection of both nations' citizens has additionally been eroded post-9/11 by competing legislation such as the U.S. Patriot Act.

The New York Times has reported that the National Security Agency in Maryland, via its worldwide operation, Echelon, intercepts 650 million messages a day. Some of these are Canadian calls and e-mail.

Mark Rasch, former head of the computer-crimes division at the U.S. Justice Department, has said that if Canadians have a problem with that, “we would have two words for them, and the second one would be ‘you.' ”

The NSA taps undersea fibre-optic cables as well.

The agency looks not for message content, but for “networks”: contacting and contacted numbers or e-mail addresses, the time and length of exchanges, and patterns — whether, for instance, someone contacted went right on

to contact someone else.

The FBI used to search for content with Carnivore, a packet-sniffer that parked itself at Internet portals to look at e-mail going through.

Carnivore nosed out key words (“bomb,” “drugs”), grabbed the mail hosting them and stockpiled it for analysis. Now, the bureau uses Magic Lantern, looking only for encrypted e-mail in order to deal more efficiently with far less volume.

Lantern is a “key logger” that records computer keystrokes. Similar software is marketed widely on the Internet to men wanting to spy on their wives, and some businesses use it to evaluate their employees' computer use.

The FBI likes key logging because keystrokes disclose passwords, PINs and encryption keys, averting the need for decryption. Its version is reportedly deployed as a virus or a Trojan horse, an innocent-seeming program that collects data from you invisibly.

After the FBI acknowledged in 2001 that Magic Lantern existed, anti-virus-software makers such as Symantec and McAfee assured customers that they were defending against it, all the while assuring the bureau that they were not.

There's no escaping CALEA or Echelon. Your $2,000 scrambler won't help you there, even a little. For now, the government's technology will always trump yours.