Wireless Interception

A look at the legalities of intercepting wireless video signals

By Elliott Goldstein

Q Is it legal to intercept wireless video signals?

A That depends on whom you ask. Most lawyers who practise criminal law (hence "criminal lawyers" – no pun intended) will tell you that the Canadian *Criminal Code* does not make it an offence to intercept video signals.

It is illegal, however, to intercept wireless (cellular) telephone signals. For example, section 184.5 makes it an offence to "intercept ... maliciously or for gain, a radio-based telephone communication, if the originator of the communication or the person intended by the originator of the communication to receive it is in Canada...."

As well, section 193.1 makes it an offence to "wilfully use or disclose a radio-based telephone communication...." A radio-based telephone communication is defined, in section 183, as "any radiocommunication within the meaning of the *Radiocommunication Act*, that is made over apparatus that is used primarily for connection to a public switched telephone network;...."[1]

Notwithstanding the above, the interception (tapping) of video-only (that is, no audio) signals from a wireless camera is not prohibited under the *Criminal Code* at this time.

If you ask a telecommunications lawyer though, he or she will refer you the *Radiocommunication Act*, section 9(2), which reads as follows: "Except as prescribed, no person shall intercept and make use of, or intercept and divulge, any radiocommunication, except as permitted by the originator of the communication or the person intended by the originator of the communication to receive it." Section 10 of that Act makes it an offence to "without lawful excuse,..., operate or possess any equipment or device, or any component thereof, under circumstances that give rise to a reasonable inference that the equipment, device or component has been used, or is or was intended to be used, for the purpose of contravening section 9...."

Why the concern with the interception of video signals from wireless surveillance cameras? According to a recent article that appeared in *The New York Times*:[2] "Thousands of people who have installed a popular wireless video camera – known as the Amazing X10 Camera – Model Xcam2X and costing about $80 – intending to increase the security of their homes and offices, have instead unknowingly opened a window on their activities to anyone equipped with a cheap receiver. The wireless video camera, which is heavily advertised on the Internet, is intended to send its video signal to a nearby base station, allowing it to be viewed on a computer or a television. It transmits an unscrambled analog radio signal that can be picked up by receivers sold with the cameras. Unfortunately, the aforementioned signal can be intercepted from more than a quarter-mile away by off-the-shelf electronic equipment costing less than $250 (USD)."[3]

"Replacing the receiver's small antenna with a more powerful one and adding a signal amplifier to pick up transmissions over greater distances is a trivial task for anyone who knows his or her way around a RadioShack store and can use a soldering iron."

The problem is that unscrupulous persons may use such a device to peek into homes where the cameras are put to use as video baby monitors, "nanny cams," or inexpensive security cameras.

At risk of detection are the wireless video cameras used by retail establishments to secretly watch their employees or customers. Worse yet, imagine the problem faced by law enforcement agencies or private investigators whose surreptitious installations of (unscrambled) wireless video cameras can be detected by criminals or suspects armed with the right equipment.

"The vulnerability of wireless products has been well understood for years. The radio spectrum is crowded, and broadcast is an inherently leaky medium."

For example, we have all heard the stories of baby monitors that would sometimes receive signals from baby monitors in neighbouring homes, from wireless home intercoms, or from early cordless phones. To prevent such monitoring, nowadays most cordless phones are scrambled.

As a result of amendments made to Part VI of the *Criminal Code*, it is now illegal under Canadian criminal law to intercept private communications made on cordless and cellular phones. This section does not apply to wireless video cameras.

This problem of unauthorized interception of wireless video signals has been variously described as "video snooping" or "video eavesdropping," "video tapping" or, less accurately, "digital peeping." Whatever label is used to describe this problem, it is a "cause for concern," says Aviel D. Rubin, a security researcher at AT&T Labs, who, in *The New York Times* article, is credited as having identified the problem.

When interviewed by that paper, Rubin said he was concerned about the kinds of mischief a criminal could carry out by substituting one video image for another. He gave as an example a robber or kidnapper wanting to get past a security camera at a locked front door of a residence.

First, the robber would secretly record the video image of a trusted neighbour knocking. Later, the robber could force that image into the victim's receiver with a more powerful signal, tricking the homeowner into thinking it was the neighbour at the door. Illegal entry would be gained when the homeowner unlocked the door, unwittingly permitting the invasion of his residence. Farfetched? Maybe, but frightening nevertheless.

In a recent column in *Canadian Security* magazine, the proposed amendments to the Canadian *Criminal Code* that would create an offence of "criminal voyeurism" have also been discussed.[4] Some American states "have (already) passed laws that prohibit placing surreptitious

cameras in places like dressing rooms, washrooms, et cetera, but American legislatures have generally not considered the legality of intercepting those signals. Nor have they considered that the signals would be intercepted from cameras that people planted themselves."

Of course, wireless video cameras equipped with scramblers or encryption technology are far less vulnerable because the content of their signal is unintelligible to persons who do not have the proper decryption or unscrambling technology to make sense of the intercepted signal. Some manufacturers do sell cameras that offer encrypted transmission, but each camera costs at least $350 USD.

Surveillance professionals who use wireless video cameras are no doubt aware of the aforementioned problem. However, awareness of this problem may not be as high among those in the alarm and security industries that sell and install wireless video surveillance cameras. It would be prudent for resellers and installers to warn their clients of the potential for interception of wireless signals from video surveillance cameras. In fact, any contract for the sale and/or installation of wireless video surveillance equipment should contain such a warning, and a limitation of liability clause.

Elliott Goldstein, BA, LL.B, is a barrister & solicitor and visual evidence consultant based in Toronto, Ontario.

Author's Notes

1 "Radiocommunication" ... means any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by means of electromagnetic waves of frequencies lower than 3,000 GHz propagated in space without artificial guide. See *Radiocommunication Act*. R.S., 1985, c. R-2, s. 1; 1989, c. 17, s. 2.

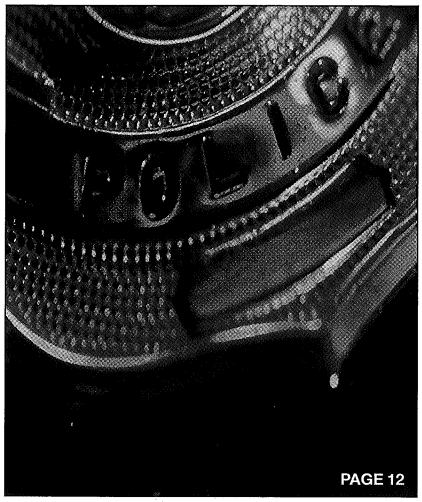
2 "Nanny-Cam May Leave a Home Exposed," by John Schwartz, *The New York Times*, April 14, 2002. All quotes are from *The New York Times* article unless otherwise indicated. Special thanks to Paul Lear for bringing this newspaper article to the author's attention.

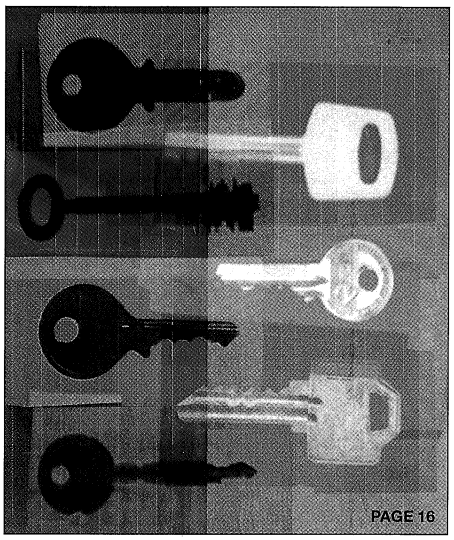
3 The device in question is advertised as the "Amazing X10 Camera – Model XCam2" and is sold on the Internet by X10 Wireless Technology of Seattle, Washington.

4 See "Sexual Spying," *Canadian Security*, December 2001, pp. 16-17.

Contents

CANADIAN SECURITY
THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT
June/July 2002 • Volume 24 Number 5





PLUS

CCTV 2002

Canadian Security's third annual 24-page pullout supplement covering CCTV issues from a range of views
By Marc Deschamps, Jacques Gagnon, Elliott Goldstein, Dave Herrington, Stacey Hunt and Peter Rollins

In Each Issue