

Observations in Education

What the video surveillance in school guidelines from Ontario's privacy commissioner could mean to you **By Elliott Goldstein**

Back in April 2002, there appeared a CCTV and the Law column entitled "Proposing Privacy," which was based on October 2001 guidelines for using video surveillance cameras in public places, as issued by Ontario's Privacy Commissioner.¹ That



publication was specifically concerned with surveillance of public places (that is, open spaces). It wasn't intended to, and didn't, deal with privacy concerns that arise in buildings such as schools.

Fairly recently, however, Ontario Privacy Commissioner Dr. Ann Cavoukian issued new guidelines specifically aimed at schools and school boards that use video surveillance cameras.² These guidelines – which are reasonable and actually make sense – are outlined below.

STUDENTS AND STAFF

Not surprisingly, the emphasis in these guidelines is the protection of privacy of students and teaching staff. According to Ontario's privacy commissioner: "[T]hese guidelines were created to assist school boards intending to use video surveillance to introduce these programs in a manner that ensures stringent privacy controls."

The guidelines acknowledge that video surveillance is useful in accomplishing three main goals:

- (1) enhancing students and staff safety;
- (2) protecting school property against theft or vandalism; and

- (3) aiding in the identification of intruders and of persons breaking the law.³

Ontario, like other provinces, has freedom of information and protection of privacy legislation. That applies to the municipal school boards and provincial schools operated directly by Ontario's Ministry of Education.⁴ Both public and separate school boards fall within the definition of "institution" found in these acts. The aforementioned privacy legislation provides rules to be followed by schools and school boards with respect to the collection, use, disclosure, retention, security and disposal of personal information.

According to Ontario's privacy commissioner: "[T]hese guidelines have been developed to apply to situations where permanent video surveillance cameras have been placed on school property. It is also important to note that the guidelines do not apply to 'covert surveillance.' Covert surveillance refers to surveillance conducted by means of hidden devices, without notice to the individuals being monitored."

Interestingly, "the guidelines will apply in any instances where a school board has set up permanent cameras to monitor students, including instances where cameras are used in school buses." Ontario's privacy commissioner recommends school boards ensure that the service providers with which they have entered into agreements are adhering to the guidelines.

OUTLINING THE ISSUES

The guidelines deal with many issues, including the following:

- collection of personal information using video surveillance;
- how to decide whether to use a video surveillance system;
- developing the school board policy for video surveillance;

- procedures governing the use, disclosure, retention, security and disposal of video surveillance records;
- access to personal information; and
- auditing and evaluating the use of video surveillance.

However, of greatest interest to you as a security professional is the section that deals with designing, installing and maintaining video surveillance equipment. In this section, the privacy commissioner sets out factors to be considered by a school board when designing a video surveillance system and installing equipment (see Editor's Note on page 10). Many of these factors are just common sense (for example, no surveillance of areas where persons are attending to personal hygiene or disrobing).

You still need to be careful about installing audio devices, though. Remember that it's illegal to intercept a private communication without consent. As well, signage should be posted in multiple languages (for example, English, French, Chinese, Italian, Spanish, Punjabi and Urdu).

Regular maintenance is also important. Certainly equipment should be checked in late August (before the school year commences) and again in early January of the following year. Checks in late April and late June, just before the summer break, are also advisable.

COVERT COVERAGE

The guidelines conclude with an appendix that addresses the issue of covert surveillance. Clearly, the privacy commissioner believes this type of surveillance should be used sparingly, and only as a last resort. The appendix, in its entirety, states the following:

"Covert surveillance occurs wherever surveillance cameras are set up without notification. Because covert surveillance takes place without notice to the public, individuals will not generally be aware

that they are being monitored. As such, the practice of covert surveillance is one that has the potential of being highly privacy-invasive and should only be used as a last resort in limited case-specific circumstances. Prior to deciding to use covert surveillance, a school board should conduct a comprehensive assessment of the privacy impacts associated with the implementation of such a program. In all cases, where it takes place, covert surveillance should be time-limited.

"The purpose of the assessment is to ensure that covert surveillance is the only available option under the circumstances and that the benefits derived from the personal information obtained far outweigh the violation of privacy of the individuals observed.

"An example of a situation in which time-limited covert surveillance may be justified is where there is an ongoing problem of computer theft from the school's computer room. If other investigative techniques have been attempted, and have failed, the school may decide to install covert surveillance equipment in order to identify the thief. Such camera equipment should be positioned in a way that minimizes surveillance (that is, the camera

should be positioned so that individuals will only be recorded if they approach the computer equipment). After a suspect has been identified, the surveillance equipment should be removed.

"A school board that uses covert surveillance as a case-specific investigation tool may consider developing, as part of sound privacy protection practices, a protocol that establishes how the decision to use covert surveillance is made on a case-by-case basis. The protocol should also include privacy protection practices for the operation of the system."

While you may not agree with all of the privacy commissioner's recommendations, you will no doubt appreciate the effort that has gone into drafting these guidelines. Hopefully, Canada's new federal privacy commissioner will follow the good example set by Ontario's privacy commissioner and draft similar guidelines for surveillance governed by both the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. ★

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

Editor's Note: To view the "Guidelines for Using Video Surveillance Cameras in Public Places (October 2001)" and a brief summary of video system design and installation for schools, visit www.canadiansecuritymag.com and click on Web Exclusives.

Author's Notes

- 1 See "Guidelines for Using Video Surveillance Cameras in Public Places (October 2001)," available at www.canadiansecuritymag.com under the Web Exclusives tab or by visiting www.ipc.on.ca. Also see British Columbia's "Public Surveillance System Privacy Guidelines," dated January 26, 2001, available at www.oipcbc.org, and Alberta's "Guide to Using Surveillance Cameras in Public Areas," dated April 2001 and available at www.oipc.ab.ca.
- 2 See "Guidelines for Using Video Surveillance Cameras in Schools (December 2003)," available at www.ipc.on.ca.
- 3 All quotes are from the guidelines cited in footnote 2, unless otherwise indicated.
- 4 See the *Municipal Freedom of Information and Protection of Privacy Act* and the *Freedom of Information and Protection of Privacy Act*.

INTRODUCING A NEW WAY TO MANAGE VIDEO

Dedicated Micros brings remote monitoring and control to your desktop with its **new network video server**. **DV-IP** stands for **Distributed Video with Internet Protocol**. DV-IP combines digital video multiplexing, digital recording, and network transmission.

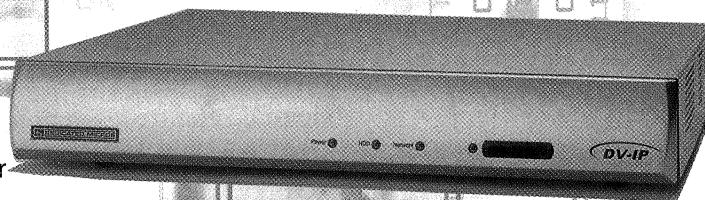
- Provides video that can be viewed via standard web browser
- Up to 16 channels of video input
- **Up to 600 GB** of internal hard drive storage for 2 months of recording
- **Advanced video motion detection** reduces false alarms
- Bandwidth limitation keeps Ethernet network operating freely
- **Webcam feature** uploads image to web server and reduces bandwidth requirements
- **Unique DuoView** allows both live and recorded images to be viewed simultaneously
- Customizable software solutions

FOR FURTHER INFORMATION PLEASE CONTACT CUSTOMER SERVICE AT 800.864.7539

NEW!

DV-IP

Network Video Server



www.dedicatedmicrosus.com

DEDICATED MICROS

April 2004 | Volume 26 Number 3

COVER STORY I

12 Show of Force

For Jim Edward, security manager for the Calgary Airport Authority, protecting an international airport is a matter of getting your security noticed

By Yvan Marston

SPECIAL SECTION I

18 Showcase of New Products

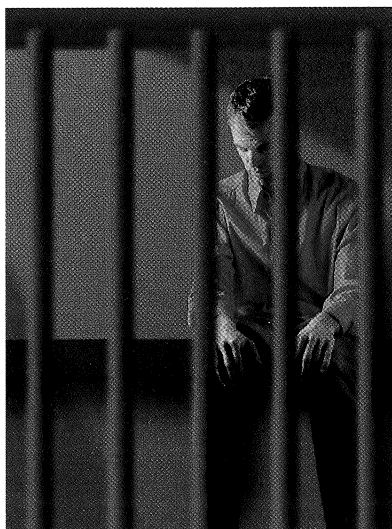
See how our independent judging panel has ranked and rewarded some of the newest innovations to hit the Canadian security marketplace

FEATURE I

26 Holding Cells and Healthcare

Whether working around prisoners or hospital patients, our experts effectively illustrate the unique and daunting challenges you'll face

By Jack Kohane



COVER: MICHELLE RAMBERG / ROTH AND RAMBERG / ANNA GOODSON



DEPARTMENTS I

4 Editor's Notebook
Hidden Agendas?

6 Industry Updates
Guidelines for CSOs; survey on security salaries; kudos to the King; and more

8 CCTV and the Law
Observations in Education
By Elliott Goldstein

31 IT Security
When Wrong is Right
By Michael Galin

34 Product Focus

34 Advertisers' Directory