

# Online Transmission

Looking at the legal implications of using the Internet to transmit images recorded from video surveillance cameras **By Elliott Goldstein**

The newest generation of digital surveillance cameras has a fully functional Web server built right in.<sup>1</sup> Video cabling (for example, coax) is no longer required because picture images are transmitted over an end user's existing Internet or a LAN via an Ethernet interface. Special software is installed on the hard drive of networked computers to permit video transition, recording and playback.<sup>2</sup> In addition, camera movement and function (for example, PTZ) can be controlled using computer software.

Analog surveillance cameras can also be connected to the Internet by way of a network video server, which simulta-

neously performs digital processing of images from a number of cameras. If a multiplexer is used, then it is connected between the cameras and the network video server.<sup>3</sup> Signals from analog cameras are sent along SSP (RS-485) or coaxial cable to the multiplexer, and then on to the network video server.

## AREAS OF INTEREST

The use of networked cameras raises some interesting legal questions, including who can authenticate the video images. Presumably, anyone who was watching the incident being transmitted in real time could come to court and testify that what he or she saw on his or her computer monitor and simultaneously recorded is the same as the pre-recorded images being displayed in the courtroom.

Another issue that arises as a direct result of "networking video" is that of image compression. Plugging cameras directly into a network may substantially increase the bandwidth requirements on computer cabling/wiring systems, unless a suitable compression method is adopted.<sup>4</sup> There are many video compression methods that employ various kinds of compression-decompression (CODEC) technologies such as MPEG, MPEG-1, MPEG-2, MPEG-4, H.261 and even M-JPEG.

The authenticating witness must be able to explain to the court what, if any, CODEC technolo-

gy was used, as well as how, if at all, it affects the images submitted as evidence.

Yet another issue is that of "water-marking." Simply put, this process is used to demonstrate an image has not been digitally "edited" or "enhanced." This issue has not been raised in any reported Canadian case and resulted in an admissibility ruling. However, sooner or later, it will be.

## WEIGHING THE WITNESS


Perhaps the most important thing is that the authenticating witness be familiar enough with IP technology to explain to the court the image transmission and recording process. Furthermore, the chain of custody of the evidence must be proven (that is, what happened to the images from the time they were recorded until the time they were shown in court).

Courts are still document-driven and, for the foreseeable future, keeping written logs or notes of what was done (and why) will greatly assist the court in its search for the truth. \*

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

## Author's Notes

- 1 For example, see the SANYO Network Camera, model VCC-WB2000. For more information, contact Tim Sherwood, SANYO Canada Inc., (905) 760-4012, e-mail: tsherwood@sci.sanyo.com. Or visit [www.sanyocanada.com](http://www.sanyocanada.com).
- 2 SANYO Network Archiving Software, VA-SW2000.
- 3 See, for example, SANYO Network Video Server, model VCC-SV2000.
- 4 Special thanks to Bob Stewart of Odyctek, Inc. of Burlington, Ontario, for his assistance with this issue.



Incidents

Search

Report

Frequency Distribution

Incident Classification

Incident Loss

More...


## Track. Report. Prevent.

**Get more from your data... Report on the facts—fast!**

With IRIMS®, PPM 2000's Incident Reporting and Investigation Management software, you'll know what's happening and where... who's involved and how. Use IRIMS' powerful reports to limit your liability, control insurance costs and meet all regulatory requirements.

**See IRIMS® in action...**  
**Call for a personalized, online demonstration.**

[www.ppm2000.com](http://www.ppm2000.com)  
**TOLL FREE 1-888-776-9776**



## COVER STORY I

### 22 Securing Information

Focusing on computer and information security, this special section covers the benefits of merging physical and network security systems, using automated technologies to manage vulnerabilities, proactively protecting systems from worms and other threats, working to effectively secure business in cyberspace, and creating an information security policy  
*By Diana-Lynn Contesti, David Hawkins, Ken Hammond and Stacey Hunt*

## FEATURES I

### 16 Crime and Punishment – Part 2 of 2

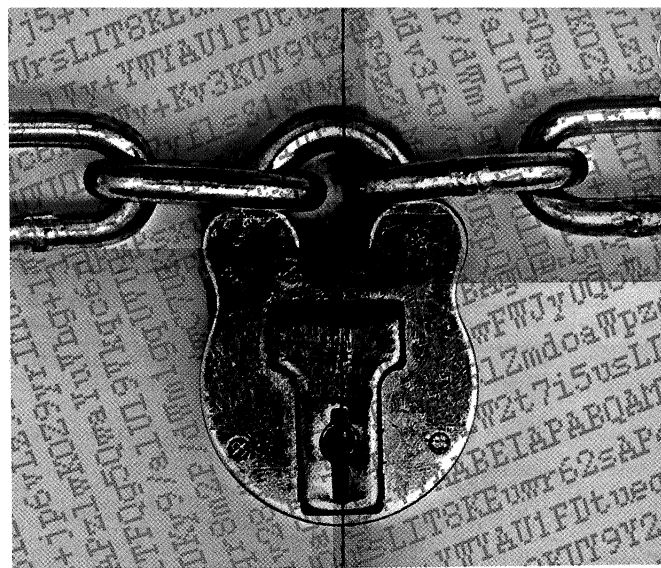
How do issues of trust unfold in a society that's being watched? When public surveillance is the issue, public education, community supports, accountability and next steps have to be reviewed *Edited by Stacey Hunt*

### 18 Ultimate Integration

Defining the benefits – and the real definition – of a truly integrated and total security knowledge management solution *By Rudy Prokupets*

### 36 Anticipating Aftershock – Part 1 of 2

Realizing the potential legislative impact of forthcoming privacy legislation *By Dean P. Davison*



## DEPARTMENTS I

### 4 Editor's Notebook

Bittersweet Remembrance

### 6 Letters to the Editor

Out with the old, in with the new

### 8 Industry Updates

Keys to effective information security; new uniform for screening officers; industry entrepreneurs make short list; and more

### 12 Alarm News

Assessing advanced security in Canada; new audio command centre; a fond farewell; and more

### 14 CCTV and the Law

Online Transmission  
*By Elliott Goldstein*

### 40 ASIS Offering

Procedure Development  
*By Herby Duverné*

### 42 Viewpoint

Risking Reputation  
*By Roger Miller*

### 44 Books & Tapes

### 45 Product Marketplace

### 45 Advertisers' Directory

### 46 Q & A

In Search of Security  
*An Interview with Roger Maslen*