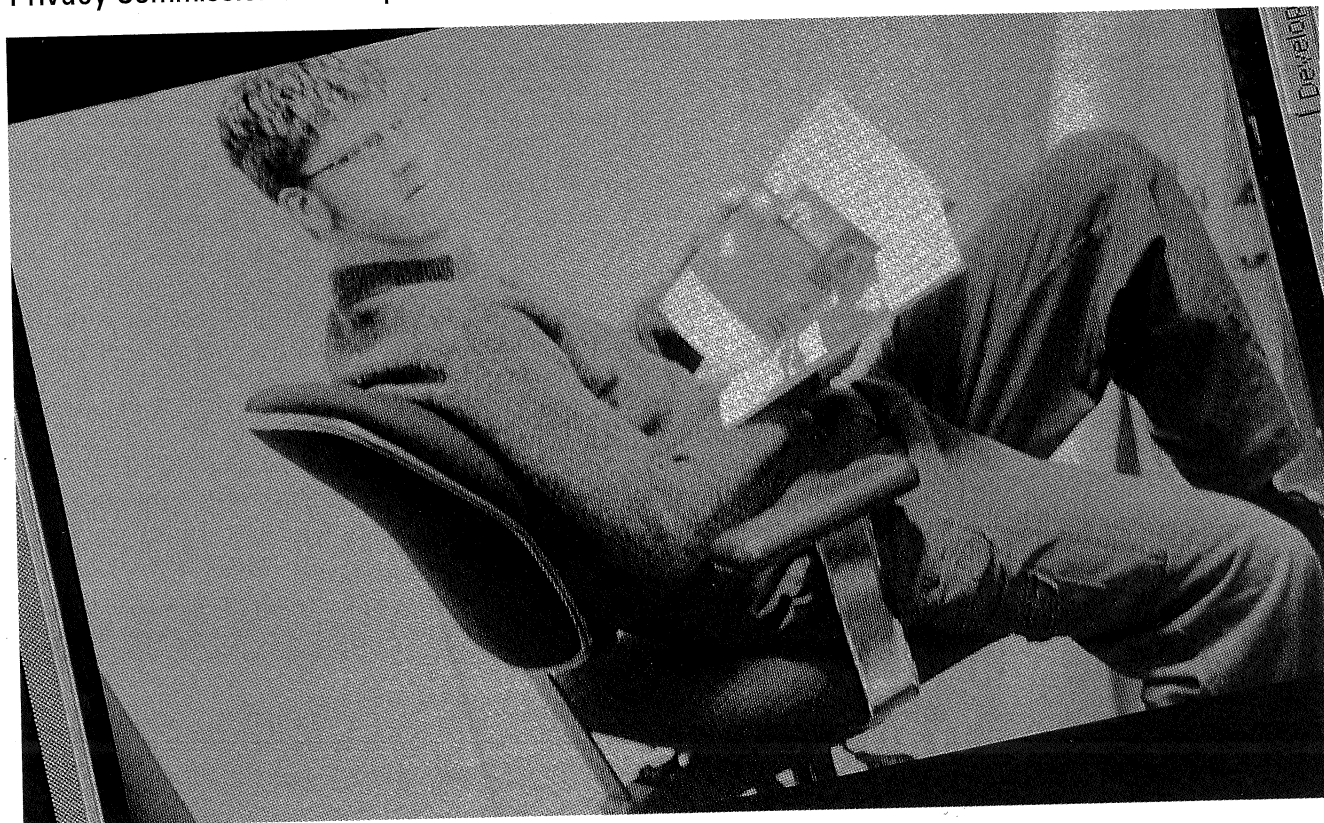


Web cams in the workplace: For security or monitoring employee performance?

Privacy Commissioner rules presence of cameras was "stifling". By Elliott Goldstein



Q Is it legal to monitor your employees over the Internet using Web cameras?

A As far as Canada's federal criminal legislation is concerned, it is not a criminal offence to conduct video surveillance of your employees without their consent.¹ However, privacy legislation, both federal and provincial, may restrict or prohibit this practice. The fact that you are using Web cameras to transmit photos or videos over the Internet is not a factor that affects the legality of the surveillance.

In a recent decision², the federal Privacy Commissioner recommended to an Internet Service Provider (ISP) that it remove the Web cameras from the sales/marketing and

technical support areas of its offices.³ The ISP, whose staff were on duty 16 hours per day during the week and 10 hours per day on weekends, installed the cameras to monitor the performance (i.e., work habits) of its employees when a manager was not on site. The ISP also argued that the cameras were needed to deter theft and harassment, and to help manage employee productivity.

The non-recording cameras were fixed into position with no pan or zoom function. Notwithstanding their low resolution, the cameras were able to capture, in sharp focus, persons within their field of view. The cameras were not placed at the main entrance or any exit from the building.

The employer posted notices advising the employees that cameras might

monitor the area in question. After installing the cameras, the employer issued a policy statement on privacy in the workplace explaining the purposes of the cameras. Each employee signed an acknowledgment that he or she had read and understood the privacy policy. Any employees who were uncomfortable with the idea of being continuously viewed had the option of working behind a movable partition.

The existence of the cameras was well known to the employees. In fact it was a former employee who complained to the federal Privacy Commission.

The Privacy Commissioner had to determine whether the employer had achieved a balance between the right to privacy of individuals and the employer's need to collect, use or disclose personal information. The Privacy

Commissioner considered the appropriateness of the employer's stated purposes (i.e., ensure security and manage worker productivity). With regard to the security issue, unauthorized entry to the facility did not appear to be the primary issue of concern since there was no camera posted at the entrance or exit points to the workplace.

The Privacy Commissioner was not satisfied that the employer presented evidence that problems such as theft and harassment were so common, and compelling that they justified the introduction of such a "privacy-invasive measure." Therefore, the Privacy Commissioner concluded a reasonable person would not likely consider security an appropriate purpose in these circumstances.

The Privacy Commissioner was also concerned about the appropriateness of intruding upon the privacy of all employees just because a few employees posed problems for management. Therefore, she considered it unlikely that a reasonable person would consider employee productivity an appropriate reason to use video and

audio surveillance.

The Privacy Commissioner commented that it appeared that the underlying purpose for the cameras really appear to be one of deterrence — deterrence of theft, harassment, malin-gering, criticism, or other behavior an employer may not like. The commissioner felt that privacy intrusive measures could always fulfill such objectives at minimal financial cost. However the PIPED Act demands that the cost to human dignity form part of the equation. The commissioner was opposed to continuous, indiscriminate surveillance of employees. She felt that omnipresent observation was stifling.

In conclusion, the Privacy Commissioner found that in the circumstances of this case she could not support the use of cameras to monitor employees at work. The complaint was well founded and the ISP was told to remove the cameras. The author of this article does not know whether the ISP complied.

The workplace in question was the offices of a private sector company, not a retail environment (store or warehouse). The area under surveillance

was not open to, or frequented by, the general public or delivery persons. Money and inventory were not handled in the area being watched.


The Privacy Commissioner's decision was obviously based on the conditions existing at the workplace in question. So, this decision should not be interpreted to mean that Web cameras are illegal or that workplace cameras are prohibited. However, this decision is indicative of the attitude that the Privacy Commissioner has to the monitoring of the performance of employees in the workplace. ★

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

¹ Assuming that no sound recordings are made of employees' communications — that is contrary to the audio surveillance sections of the *Criminal Code*

² PIPED Act case summary [#279] issued July 26, 2004 available from www.privcom.gc.ca.

³ The Privacy Commissioner does not have law-ordering or law-enforcement powers. However, the Federal Court can be used by the person who filed the complaint with the Privacy Commission to enforce the Commissioner's findings if the Federal Court judges rule in favour of the complainant.



Incidents
Search

Report
 Frequency Distribution
Incident Classification
 Incident Loss
 More...


Track. Report. Prevent.

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


IRIMS®, PPM 2000's Incident Reporting and Investigation Management software, is a turnkey solution that streamlines processes, limits liability and reduces costs.

See IRIMS® in action...
 Call Susan Kedzo, PPM's Regional Account Manager for Canada, to arrange a personalized demonstration.


TOLL FREE 1-888-776-9776



www.ppm2000.com




Armour Shield Plus Glass Laminates



Protecting you from:

- Natural Disaster
- Accidental Damage
- Human Threat

Vandalism and Smash & Grab crimes are on the rise. Let Armour Shield Plus with over 20 years of installation experience protect your employees and property. Armour Shield Plus glass laminates is a deterrent to both vandals and thieves.



Armour Shield PLUS Inc.

61 Alness, Unit #221, North York
 Ontario, Canada M3J 2H2
 tel: 416-667-8468 or 1-866-668-8846
 fax: 416-663-8676

SAVE MONEY - FACTORY DIRECT PRICING

January / February 2005 | Volume 27 Number 1

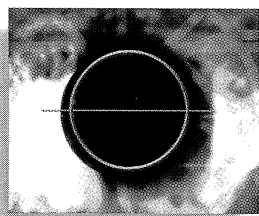
COVER STORY I

20 From Ship to Shore

Graham Kee, director of security for the Vancouver Port Authority, watches over one of Canada's major economic hubs.

By Jennifer Brown

FEATURES I



24 Not Just Spyware Anymore

Canada's Air Transport Security Authority clears biometric technology for landing.

By Vawn Himmelsbach

28 Bridging the Gap

The St. Lawrence Seaway upgrades its CCTV system with improved technology for remote surveillance.

By Jack Kohane



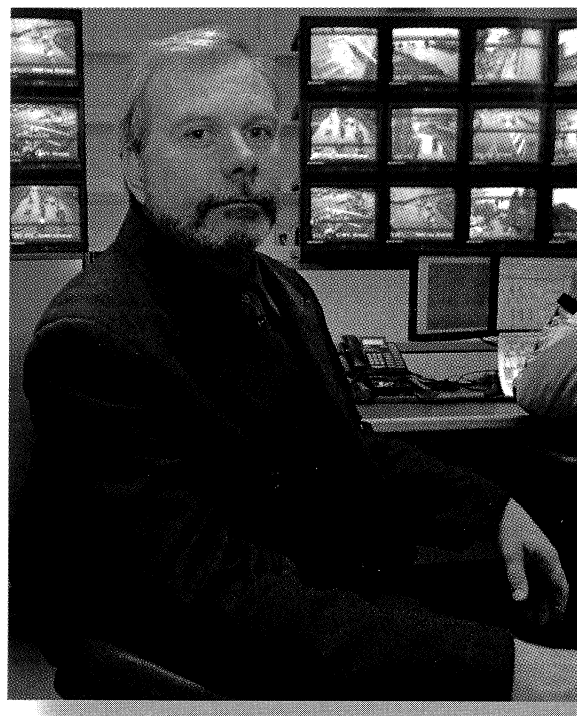
32 Training as a Security Management Tool

A little time in the classroom can improve quality of service and reduce employee turnover.

By Jody Reid

38 2005 ANNUAL DIRECTORY & BUYERS' GUIDE

Canada's most comprehensive resource for finding security products and services in print and online at www.canadiansecuritymag.com



COVER: KIM STALLKNECHT

DEPARTMENTS I

6 Editor's Notebook

In transit

8 Letters to the Editor

Ending the cycle

10 Industry Updates

Ontario introduces long-awaited changes to private security and investigators Act; Security screeners at Ottawa airport ratify agreement; Commissionaires win contract at B.C.'s Big White Ski Resort

16 Books and tapes

Rethinking Corporate Security in the Post 911 Era; Issues and Strategies for Today's Global Business Community; A Security Professional's Practical Guide to the Law

18 CCTV and the Law

Web cams in the workplace: Was the intention security or monitoring employee performance?
By Elliott Goldstein

34 IT Security

Create an enterprise security strategy
By Nick Galletto

36 From the Trenches

Runway Hit
By Tony de Santana

Subscriber Services

240 Edward Street, Aurora, Ontario L4G 3S9 (905) 727-0077 • Fax (905) 727-0017

I.S.S.N. 0709-3403 Printed in Canada

Canada Post: Customer #1939416, Agreement #40063602.