Law of the Month: BC Lays Down Privacy Guidelines for Workplace Surveillance Cameras

Video surveillance can help you keep the workplace secure. But it can also get you into big trouble under privacy laws. The key for employers is to steer a middle course between legitimate security and respect for the individual privacy of employees and third parties who may come under the cameras' lenses. New government guidance explains how to keep workplace video surveillance within privacy bounds. And while the Guidance comes from BC, the same principles apply in all parts of Canada.

OVERVIEW OF THE GUIDANCE

What the Law Says: Privacy laws ban the collection and use of personal information without the individual's consent. Footage captured by surveillance cameras is considered personal information protected by the law. However, authorization is *not* required if collection and use serve a legitimate purpose, such as workplace security, as long as you limit things to collections and uses that are reasonably necessary to accomplish the legitimate purpose.

What the Guidance Does: The Guidance explains how these principles apply to use of surveillance cameras in the workplace.

What the Guidance Says: According to the Guidance, workplace video surveillance is a highly intrusive technology and should be used only as a measure of last resort. The Guidance instructs employers not to use video surveillance unless and until they make 3 determinations:

- The problem is serious enough to warrant use of surveillance cameras;
- Surveillance cameras will be effective in solving the problem; and
- The problem can't be resolved via use of alternatives that are less invasive of privacy.

10 THINGS TO DO

The Guidance lists 10 things to do to minimize the privacy impact of workplace video surveillance.

1. **Implement a Surveillance Policy**

First you need a written workplace video surveillance policy that explains, at a minimum:

- The purpose of surveillance;
- Your determination that surveillance was necessary to accomplish that purpose;
- When and how monitoring and recording will take place;
- How recordings will be used and how long they'll be retained;
- The procedures for secure disposal of the recordings; and
- A process to follow in the event of an unauthorized disclosure.

2. **Limit Time of Surveillance**

Workplace video surveillance limited to particular times of the day or night is preferable to keeping the cameras on 24/7, according to the Guidance.

3. **Limit Time of Surveillance**

Take steps to minimize the risk of filming individuals who aren't targets of surveillance, e.g., by positioning cameras in places where they won't capture pedestrians and avoiding areas like bathrooms in which people have heightened expectations of privacy.

4. **Post Warning Signs**

Post a clear, understandable notice about the use of cameras before people enter the workplace and at entrances to areas that are under surveillance. Signs should indicate plainly which area is under video surveillance and for what purpose, for example: "This property is monitored by video surveillance for theft prevention." They should also list contact information for individuals to go if they have questions.

5. **Securely Store Recordings**

Like any other confidential information, surveillance equipment should be securely stored to prevent unauthorized access and removal.

6. **Establish Secure Retention and Destruction Procedures**

Don't keep recordings longer than necessary—the Guidance recommends a 30 days' maximum. Make sure you destroy recordings in a secure manner when you no longer need them.

7. **Establish Access Limits**

Your workplace video surveillance policy should specify the individuals authorized to access recordings. Limit access to specific purposes, e.g., to investigate significant security or safety incidents. Use technological controls like password and user authentication to effectuate access limits and keep logs documenting access requests and usage.

8. **Provide Open Access to Your Surveillance Policy**

The Guidance recommends making your surveillance policy available to the public. "Your customers will appreciate your transparency and gain a better understanding of the purposes of the surveillance."

9. **Respect Subjects' Right to Access Footage**

Under privacy laws, you must grant individuals that you film access to the footage in

which their images are captured, provided that they request it. When disclosing recordings, use masking technology to avoid inadvertently revealing identifying information about other individuals on the tapes.

10. **Periodically Re-Evaluate Your Need for Surveillance**

Regularly review your policy to verify that using workplace video surveillance is still justifiable and needed for your original purpose.

Caveat: Open, Not Covert Surveillance

One last thing to keep in mind: The Guidance addresses overt surveillance where cameras are in the open, warnings are posted or subjects are otherwise made aware that they’re being recorded; rules governing covert or secret surveillance are much stricter.