updated December 2016

Guide to using overt video surveillance

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Implementing Overt Video Surveillance

Installing surveillance equipment may seem like a logical decision for your organization, but unauthorized collection and use of personal information through video surveillance could lead to violations of B.C. privacy laws and create other costly liabilities.

Video surveillance should only be used as a last resort after exhausting other less privacy-invasive alternatives, such as improved workplace supervision or financial controls. As well, organizations need to consider whether video surveillance will achieve the intended purpose and whether the issues you are experiencing are serious enough to warrant implementing this highly invasive technology.

If collecting personal information via video surveillance is necessary and authorized under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") or the *Personal Information Protection Act* ("PIPA"), consider these steps before you install the system:

1. Develop a surveillance policy

Your video surveillance policy should, among other things, explain the rationale and purpose of the surveillance; when and how monitoring and/or recording will be in effect; how recordings will be used; retention periods; procedures for secure disposal of the recordings; and a process to follow if there is an unauthorized disclosure.

2. Limit the time your surveillance is active

Cameras that are live for certain times of the day or night are preferable to those that are turned on 24/7. So only monitor or record during the time period that meets your specific purpose. For instance, if you operate a retail store and have experienced break-ins after hours, only use your cameras when the store is closed, so you are not capturing images of employees and customers.

3. Avoid unintended subjects

One of the unexpected consequences of video surveillance is that cameras can easily capture images of people who are not targets, which would not be authorized under FIPPA or PIPA.

- Position cameras to reduce unauthorized image capture. For example, a store security camera should not capture images of passersby on the street.
- Avoid areas where people have a heightened expectation of privacy, such as change rooms, washrooms, or into windows.

4. Use adequate signage to notify the public

Post a clear, understandable notice about the use of cameras *before* your clients or customers enter the premises and at the entrances to different areas within your property that are under surveillance (e.g.: parking lot). Notification is respectful of their privacy, gives them the option not to enter, and is required by law.

The sign 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.” It should also provide contact information for someone in your organization if individuals have questions about the surveillance.

5. Store any recorded images in a secure location

Surveillance equipment should be stored under lock and key, to protect your employees, guests, customers, and clients—and your organization—from the risks of a privacy breach. Don’t remove images from your premises and always follow a strict storage protocol.

6. Destroy recorded images when they are no longer needed

Prepare a retention and destruction schedule to specify the length of time that surveillance records will be kept (we recommend a maximum of 30 days). Decide when and how records will be destroyed. Safely and securely destroy recorded images when they are no longer required for business purposes. Document the destruction in your logs.

7. Limit access to recorded images to authorized individuals

Your video surveillance policy should identify who is authorized to access the recordings. You should only review the recorded images to investigate a significant security or safety incident, such as when you have reported a crime to the police. Make sure that the right training is provided to your operators on an ongoing basis, so that they know their obligations under all relevant legislation. Minimize the number of individuals who have access to the system, monitoring, or recordings.

Any disclosure of video surveillance recordings outside your organization should be authorized by the applicable privacy law and documented.

8. Open access to your surveillance policy

Consider making your written surveillance policy available to the public. Your customers will appreciate your transparency and gain a better understanding of the purposes of the surveillance.

9. Consider right of access

Anyone whose image is captured by your surveillance video has the right to access their own personal images, so you must be prepared to provide a copy of the relevant surveillance recording upon request.

When disclosing recordings, use masking technology to ensure that identifying information about other individuals on the recording is not inadvertently revealed.

10. Periodically re-evaluate your need for video surveillance

Organizational needs change. Regularly review your policy to ensure that using video surveillance is still justifiable and needed for your original purpose.

These guidelines are for information only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia with respect to any matter within the jurisdiction of the Freedom of Information and Protection of Privacy Act ("FIPPA") or the Personal Information Protection Act ("PIPA"). These guidelines do not affect the powers, duties or functions of the Information and Privacy Commissioner regarding any complaint, investigation or other matter under or connected with FIPPA or PIPA, respecting which the Information and Privacy Commissioner will keep an open mind.