Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

GUIDANCE DOCUMENT

USING OVERT VIDEO SURVEILLANCE

OCTOBER 2017

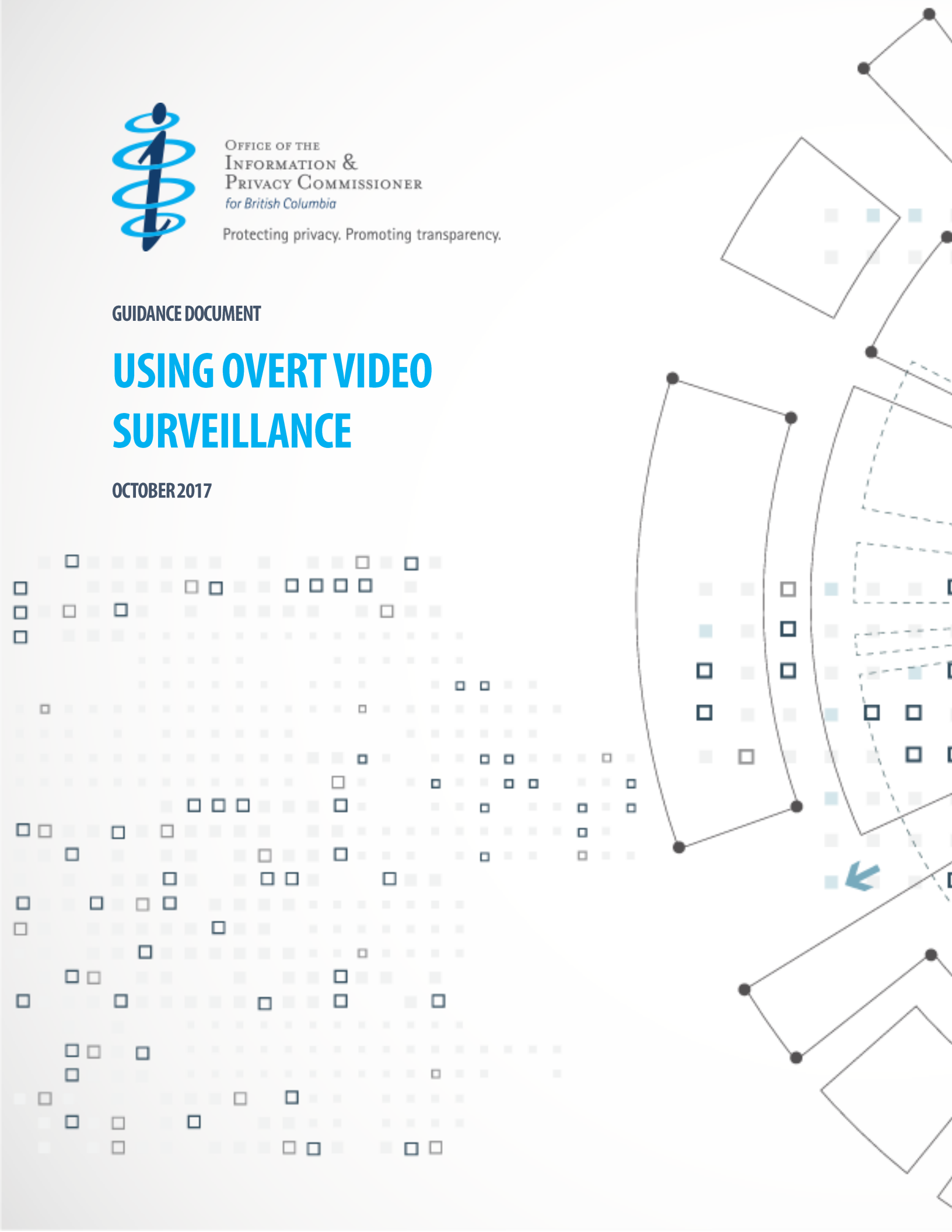

TABLE OF CONTENTS

PURPOSE OF THIS GUIDANCE DOCUMENT

This guide is for public bodies and organizations that are interested in using video surveillance in compliance with BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). It recommends privacy protective measures that should be considered prior to installation of video surveillance systems.

APPROPRIATE USE

Installing surveillance equipment may seem like a logical decision for your organization, but collection and use of personal information through video surveillance may violate BC privacy law and could lead to other costly liabilities.

Video surveillance should only be used as a last resort after exhausting less privacy-invasive alternatives, such as improved workplace supervision or implementation of theft-prevention controls. Organizations need to consider whether video surveillance will achieve the intended purpose and whether the concerns are serious enough to warrant implementing this highly invasive technology.

POLICIES AND PROCEDURES

If collecting personal information via video surveillance is necessary and authorized under the legislation, you will need to develop appropriate policies and procedures. Your video surveillance policy should explain the rationale and purpose of the surveillance; when and how monitoring and/or recording will be in effect; how recordings will be used; for how long they will be kept; how they will be securely deleted; and a process to follow if there is unauthorized access or disclosure.

ADVICE FROM THE COMMISSIONER	Develop a surveillance policy.

LIMITED COLLECTION

The most privacy protective approach is to limit the time your surveillance is active. This means only turning on the cameras for certain times of the day or night rather than 24 hours a day, so you only monitor or record during the times that meets your specific need. 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 that you are not capturing images of employees and customers during business hours.

Another consequence of video surveillance is that cameras may capture images of people who are not the intended subjects. This would not be authorized under FIPPA or PIPA. To ensure your surveillance is lawful:

- Position cameras to capture the least amount of information that is needed. 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.

ADVICE FROM THE COMMISSIONER	Limit the time your surveillance is active.
	Avoid unintended subjects.

LIMITED ACCESS

Your video surveillance policy should identify individuals who are authorized to access the recordings. Authorized individuals should only review the recorded images to investigate a significant security or safety incident, such as criminal activity. Minimize the number of individuals who have access to the monitoring system or recordings, and ensure they have adequate ongoing privacy training so they are clear about their legal obligations.

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

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 disclosed.

ADVICE FROM THE COMMISSIONER	
	Limit access to recorded images to authorized individuals.
	Consider right of access.

SECURE STORAGE AND DESTRUCTION

Surveillance equipment should be securely stored to prevent theft of personal information and protect your employees, guests, customers—and your organization—from the risks of a privacy breach. To reduce the possibility of loss and theft, do not remove video recording from your premises and follow a secure storage protocol.

Prepare a retention and destruction schedule to specify the length of time that surveillance records will be kept (we recommend a maximum of 7 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.

ADVICE FROM THE COMMISSIONER	
	Store any recorded images in a secure location.
	Destroy recorded images when they are no longer needed.

ACCOUNTABILITY

Post a clear, understandable notice about the use of cameras that is visible before individuals enter the premises. Providing notification is respectful of their privacy, gives them the option not to enter, and is required by law. The sign must plainly indicate which areas are under video surveillance and for what purpose, for example: “This property is monitored by video surveillance for theft prevention.” It must also provide contact information of someone in your organization for individuals to contact if they have questions about the surveillance.

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 and the security measures that are in place to protect their personal information. Finally, regularly review your policy to ensure that using video surveillance is still justifiable and needed for your original purpose.

ADVICE FROM THE COMMISSIONER	
	Use adequate signage to notify the public.
	Allow access to your surveillance policy.
	Periodically re-evaluate your need for video surveillance.

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867
info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy