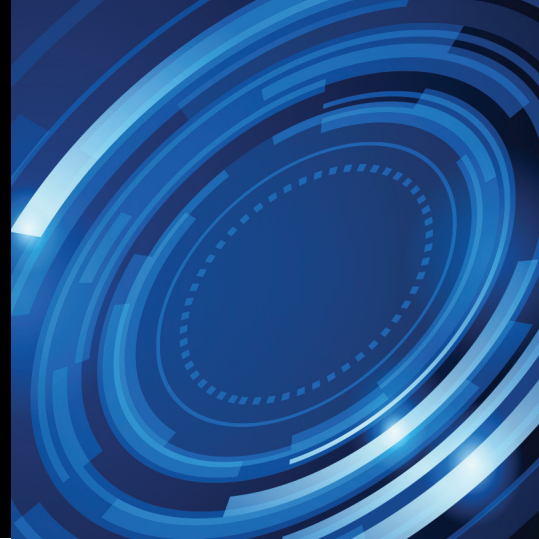


GUIDANCE FOR THE USE OF BODY-WORN CAMERAS BY LAW ENFORCEMENT AUTHORITIES



This guidance document aims to identify some of the privacy considerations law enforcement authorities should take into account when deciding whether to outfit law enforcement officers with body-worn cameras. Also described is the privacy framework that should be part of any law enforcement body-worn camera program in order to ensure compliance with Canada’s personal information protection statutes.

This document is endorsed by:

Office of the Privacy Commissioner of Canada

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner for British Columbia

Manitoba Ombudsman

Office of the Access to Information and Privacy Commissioner - New Brunswick

Office of the Information and Privacy - Newfoundland and Labrador

Office of the Information and Privacy Commissioner of the Northwest Territories

Nova Scotia Freedom of Information and Protection of Privacy Review Office

Office of the Information and Privacy Commissioner of Nunavut

Office of the Information and Privacy Commissioner of Ontario

Office of the Information and Privacy Commissioner of Prince Edward Island

Commission d'accès à l'information du Québec

Office of the Saskatchewan Information and Privacy Commissioner

Office of the Yukon Information and Privacy Commissioner



Guidance for the use of body-worn cameras by law enforcement authorities

Introduction

This guidance document aims to identify some of the privacy considerations law enforcement authorities¹ (LEAs) should take into account when deciding whether to outfit law enforcement officers with body-worn cameras (BWCs). Also described is the privacy framework that should be part of any law enforcement BWC program in order to ensure compliance with Canada's personal information protection statutes. This guidance is meant to support LEAs in developing policies and procedures governing the use of BWCs. It relates to the *overt* use of BWCs, that is, BWCs that are used in view of the public and with the understanding that the public has been informed of their deployment. The covert use of BWCs is not addressed through this guidance.

This document was developed by the Office of the Privacy Commissioner of Canada in collaboration with the privacy oversight offices in [Alberta](#), [New Brunswick](#), and [Quebec](#) and in consultation with the privacy oversight offices in [British Columbia](#), [Manitoba](#), [Newfoundland and Labrador](#), [Northwest Territories](#), [Nova Scotia](#), [Nunavut](#), [Ontario](#), [Prince Edward Island](#), [Saskatchewan](#) and [Yukon](#).


Apart from requirements under personal information protection statutes, the use of BWCs can implicate other obligations of which LEAs need to be aware. For example, BWCs can record video images, sound and conversations with a high degree of clarity. Thus, there may be additional concerns raised under the *Canadian Charter of Rights and Freedoms*, the *Criminal Code*, or provincial legislation², for example, whether the use of BWCs in any given context intrudes on the public's reasonable expectation of privacy or constitutes an interception of private communications, including in places accessible to members of the public. LEAs also need to be mindful of additional legal implications whenever images and sound are recorded in private spaces, such as inside people's homes or vehicles.

BWCs and privacy

BWCs are recording devices designed to be worn on a law enforcement officer's uniform, which can include glasses or helmets. They provide an audio-visual record of events from an officer's point of view as officers go about their daily duties. The high-resolution digital images allow for a clear view of individuals and are suited to running video analytics software, such as facial recognition. Microphones may be sensitive enough to capture not only the sounds associated with the situation being targeted but also ambient sound that could include the conversations of bystanders.

¹ This constitutes government agencies responsible for enforcing laws and includes, but is not limited to, police forces.

² For example, in Québec, the *Charter of Human Rights and Freedoms* or the *Civil Code of Québec*.



BWC technology represents a significant increase in sophistication from the early days of fixed cameras, when CCTV systems were being widely adopted and could only record images and not sound. At that time, a number of Canadian privacy oversight offices issued video surveillance guidelines for the public sector, which are set out at the end of this document. While the basic privacy principles around video surveillance remain the same, the environment is now much more complex. As surveillance technologies evolve, ever larger amounts of personal information (both video and audio) are being collected in increasingly diverse circumstances (both static and mobile) with the potential of being linked with yet other personal information (e.g. facial recognition, metadata). It is understandable that LEAs would want to consider using new technologies to aid them in performing their duties. At the same time, however, BWC technology poses serious implications for individuals' right to privacy. We believe that addressing privacy considerations from the outset can allow an appropriate balance to be achieved between the needs of law enforcement and the privacy rights of individuals.

Body-worn cameras capture personal information

Canadian personal information protection statutes generally define personal information as being “about an identifiable individual.”³ Under Québec’s *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, personal information is “any information which relates to a natural person and allows that person to be identified.”

Generally speaking, the aim of a BWC program is to record law enforcement officers’ interactions with the public in the course of their duties. BWCs are generally used for collecting evidence, and protecting officers against unfounded allegations of misconduct. Another significant argument for BWCs is enhancing officer accountability and professionalism. Given this context, and the increasing quality of recordings and sensitivity of microphones, the images and sound captured by BWCs for the most part will be about identifiable individuals. The recordings will thus be considered to contain personal information and will be subject to Canada’s personal information protection statutes.


In addition to images and sound, BWCs can also generate metadata, which can include transactional information about the user, the device and the activities taking place. Metadata can include date, time, location and duration of the recorded activities, which, when connected to an identifiable individual, can be personal information⁴.

What is the right balance between privacy and law enforcement needs?

There are various reasons why a LEA might contemplate adopting BWCs. LEAs could view the use of BWCs as bringing about certain benefits to policing or other enforcement activities. For

³ The case law at the federal level has generally held that information will be about an identifiable individual if it permits or leads to the possible identification of the individual, whether alone or in combination with other available information.

⁴ For further information on metadata, please see the Ontario OIPC’s [“A Primer on Metadata: Separating Fact from Fiction”](#) and/or the OPC’s [“The Risks of Metadata”](#)



example, in addition to being used to collect evidence, BWCs have been [associated with](#) a decrease in the number of public complaints against police officers as well as a decrease in the use of force by police officers. At the same time, BWCs have significant privacy implications that need to be weighed against the anticipated benefits. As the Supreme Court of Canada has noted⁵, an individual does not automatically forfeit his or her privacy interests when in public, especially given technological developments that make it possible for personal information “to be recorded with ease, distributed to an almost infinite audience, and stored indefinitely”. And as the Supreme Court added more recently, the right to informational privacy includes anonymity which “permits individuals to act in public places but to preserve freedom from identification and surveillance.”⁶

The use of BWCs inside private dwellings brings up special considerations, such as the higher likelihood that individuals will be recorded in highly personal situations. Before proceeding with a BWC program, LEAs should identify their lawful authority for collecting personal information using BWCs. Generally, under public sector personal information protection statutes, public bodies may only collect the information they need to meet the purposes of their mandated programs and activities. As a second step, LEAs should evaluate whether the anticipated benefits of adopting BWC technology outweigh the resulting privacy intrusions. In other words, is it appropriate to equip officers with cameras given the privacy implications they raise?

Privacy oversight offices have found it useful to use a four-part test to evaluate whether a proposed measure can be justified despite an intrusion on individual privacy. The test of “what a reasonable person would consider appropriate in the circumstances” provides a useful basis for LEAs in setting out the rationale for adopting BWCs. LEAs should be guided by this four-part test as set out below in determining whether to implement BWCs.

Necessity

There must be a demonstrable operational need that a BWC program is meant to address. What operational needs do LEAs have for which BWCs are a solution?

BWCs should not be adopted simply because they may be considered a popular enforcement tool. They must be judged necessary to address specific operational circumstances in the jurisdiction they are deployed in.

Effectiveness

Are BWCs likely to be an effective solution to the operational needs that have been identified? LEAs should be mindful of the limitations of technology. Aspects of incidents may happen out of camera range, sound recordings may be incomplete due to range or background noise, or human error may compromise the usefulness of recordings and diminish their effectiveness. If recordings are meant to be used as evidence in court proceedings, LEAs should consider the requirements identified by Courts for accepting recordings as evidence as well as the evidence collection and retention measures proposed to ensure those requirements are satisfied.

⁵ *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para. 27.

⁶ *R. v. Spencer*, 2014 SCC 43



Proportionality

Without a doubt, the use of BWCs will result in a loss of privacy because recording individuals' actions and conversations is inherently privacy invasive. As such, any privacy intrusion must be minimized to the extent possible and offset by significant and articulable benefits. With new technology, it may be difficult to foresee the full spectrum of positive and negative effects on day-to-day enforcement and the community being served. Undertaking a pilot project is highly recommended as a practical way of evaluating the privacy impacts of BWCs in relation to their benefits, before deciding whether or not to deploy them, how broadly, and in what circumstances.

Alternatives

A final consideration is whether a less privacy-invasive measure would achieve the same objectives. While there may be a business case for a BWC program, alternative measures should be considered to see whether they can adequately address operational needs with less adverse impact on privacy. The least privacy invasive measure is the preferred choice.

Privacy Impact Assessments


As a highly recommended best practice, a Privacy Impact Assessment (PIA) should be completed prior to the use of BWCs to help identify the potential privacy risks of the BWC program. A PIA can be invaluable in helping LEAs eliminate those risks or reduce them to an acceptable level. For example, there may be additional considerations, such as context and cultural sensitivities, that should be considered in deciding whether to use BWCs in particular situations. A PIA should include a plan for consulting and engaging with the community where BWCs are to be deployed.

LEAs can also seek the aid of privacy experts before implementing a BWC program. Privacy experts can study the proposed use of BWCs in the community to ensure that any collection and use of personal information is done with a view to upholding obligations under privacy legislation.

Secondary uses

Employee privacy should also be taken into account. BWCs can capture law enforcement officers' personal information, which is protected under most public sector privacy laws. Potential areas of concern include using BWC recordings to support employee performance evaluations. Employees may also have privacy rights under other laws and collective agreements that may affect a BWC program.

If use of recordings is contemplated for any purposes that are supplementary to the main BWC program purposes, for example, officer training, research, or performance evaluation, these secondary purposes need to be reviewed to ensure compliance with applicable legislation, and employees need to be well informed of them. In addition, criteria should be established to limit



the privacy impact, such as blurring of faces and any identifying marks, and excluding recordings with sensitive⁷ content.

Pilot projects

The considerations in implementing a BWC program are complex, and pilot projects are recommended as an important precursor to widespread adoption. It is generally good practice, when deploying new technologies, to try them out in the field on a limited basis. If a LEA decides that adopting BWCs is appropriate, a pilot project would demonstrate how BWCs actually perform in their specific environment and whether this technology produces useful results that satisfy the intent of the program. The pilot project could also inform the crafting of a clear policy framework, applicable training requirements, and required supervision.

Evergreening PIAs

After a BWC program has been adopted, additional PIAs are recommended as a best practice any time significant modifications to the program are contemplated. Significant modification would include a new collection of personal information and the introduction of new technologies or analytical tools.

Notifying the public


LEAs should make a reasonable effort to inform the public that officers are equipped with BWCs and that people's actions and words may be recorded when they interact with, or are in the vicinity of, law enforcement officers. Transparency is integral to the public's ability to exercise their rights under privacy laws.

Public awareness of the use of BWCs can be raised through the local media, social media campaigns, and on LEA websites. Individuals should be advised if BWCs are used, for what purpose, in what circumstances, under what authority and who they can contact in case of questions. As part of their commitment to fostering public awareness, LEAs should consider reminding the public that individuals have a right to access their own personal information, as well as a right to request access to information generally under freedom of information laws that apply to BWC recordings.

Notification is also important in encounters between law enforcement officers and the public. Should non-uniformed officers use BWCs, there is an increased risk that the public will be unaware that recording may potentially take place.

While BWCs are visible on the officer's uniform or glasses, they may not be noticed by individuals, particularly in stressful situations. Individuals also may not be aware that sound is being recorded in addition to images.

⁷ LEAs should determine criteria for designating sensitive content, with input from the affected community, and ensure a higher level of protection for such recordings.



Law enforcement officers should be required to notify people of recording both images and sound whenever possible. Officers could make a short statement that meets notice requirements under applicable legislation in their jurisdiction. A prominent pin or sticker on the officer's uniform could also be an option depending on the circumstances.

Continuous versus intermittent recording

One of the most important operational decisions LEAs must make in implementing a BWC program is whether BWCs should record continuously or whether officers should have the discretion or duty to turn them on and off, and, in either scenario, under what circumstances. These choices have important implications for privacy.

From an accountability perspective, continuous recording may be preferable because it captures an unedited recording of an officer's actions and the officer cannot be accused of manipulating recordings for his or her own benefit. However, from a privacy perspective, collecting less or no personal information is always the preferred option. The less time BWCs are turned on, the less personal information they will collect. Minimizing the personal information collected decreases the risk that personal information will be used or disclosed for inappropriate or unintended purposes. This applies both to members of the public whose personal information is recorded by BWCs as well as law enforcement officers. There may be times during an officer's workday that having the camera turned on would not capture any information related to evidence collection or any other stated purpose of the BWC program, for example, when the officer is "standing by" or doing paperwork. LEAs also have a responsibility to respect officers' personal privacy when off-duty or on personal time. As for recording the public, LEA programs should take into account situations that merit heightened privacy protections, such as when officers enter private dwellings.


In general, it will be difficult for LEAs to justify the necessity of continuous recording. Recording may be more readily justified, however, in relation to carefully defined incidents or operational requirements.

If intermittent recording is implemented, there should be strict criteria for turning cameras on and off, including criteria for determining whether the officer should have control in turning the cameras on or off, or whether this should be done remotely.

The criteria developed should take into account fundamental freedoms, human rights, cultural sensitivities and any significant concerns expressed by the affected community.

Try to avoid recording bystanders

The criteria for activating cameras should address the need to minimize, to the extent possible, the recording of innocent bystanders or innocuous interactions with the public. Admittedly, it may not be possible to completely eliminate capturing images and audio of bystanders and other non-targeted individuals. With regard to recordings that are not implicated in an investigation (i.e. non-flagged recordings), setting and respecting limited and appropriate retention periods, and restricting access and viewing to a need-to-know basis will help mitigate the privacy implications.



With regard to recordings that have been flagged for use as evidence or for another previously specified purpose, technical means should be employed to mitigate the privacy risk. Within the rules of evidence, and in particular, the jurisprudence with respect to the reliability of evidence, images of bystanders and other non-targeted individuals should be anonymized, for example, through face blurring, and the distortion of sound wherever possible.

If images and/or audio are shared with the public for the purpose of identifying someone, other persons in the images should be obscured, with measures taken to safeguard the evidentiary integrity and reliability of the recording.

Proper safeguards, retention, destruction and storage of BWC recordings


Under privacy legislation, LEAs are responsible for protecting personal information from unauthorized access or use, disclosure, copying, modification and destruction, as well as loss and theft. Reasonable steps must be taken to safeguard recordings, such as:

- encrypt recordings and store them on a secure server;
- restrict access to recordings, on a need to know basis;
- edit-proof video and audio; and,
- implement an audit trail to provide assurance that recordings have not been modified or accessed inappropriately.

LEAs contemplating storing BWC recordings in the cloud should be mindful of potential security concerns as well as any legal constraints that may apply in their jurisdiction. For example, British Columbia's *Freedom of Information and Protection of Privacy Act* and Nova Scotia's *Personal Information International Disclosure Protection Act* may not allow public bodies to store personal information outside of Canada. Québec's *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* imposes certain conditions on the storage of personal information outside the province.

In light of the significant privacy implications of BWCs, strict retention periods should be imposed, taking into account the requirements of all applicable legislation. Setting and respecting retention periods will limit any opportunities for inappropriate disclosure or misuse of the information, including the potential for monitoring individuals without reasonable suspicion or probable cause.

Retention policies for flagged recordings, including recordings to be used as evidence, should be consistent with applicable laws, such as the *Canada Evidence Act* and the applicable *Police Services Act*. Under Canada's privacy laws, personal information that has been used in making a decision affecting an individual needs to be retained for a sufficient period so as to afford individuals a reasonable opportunity to access it and challenge its accuracy. Recordings that have not been flagged as relevant to an investigation or potential legal action should have the shortest possible retention period.



When the retention period is up, recordings should be disposed of in a secure manner in accordance with applicable policies⁸ and regulations.

There should be systems in place to ensure that safeguarding, retention and destruction policies are respected.

Use of video analytics

Any plans to use video analytics in conjunction with BWCs should be carefully considered with regards to the initial justification of the program. With advances in technology, we are gaining increasing ability to search and analyze digital footage in increasingly sophisticated ways. Databases of camera footage can be mined for information about specific individuals or specific activities. Previously anonymous individuals can be identified and tracked.

Technologies such as licence plate recognition, facial recognition and pattern recognition can be used in identifying, tracking and compiling dossiers on individuals. LEAs' use of video analytics technology raises additional privacy concerns that require further scrutiny and care beyond the scope of this guidance.

At this time, we simply observe that if the use of such analytics can be justified under privacy laws, the capability to analyze recordings must be carefully managed so as not to exceed the documented purposes of the BWC program. Integrating recordings with video or audio analytics should only be considered on a case-by-case basis, under very limited circumstances to be determined by the head of the LEA involved, and subject to a new PIA as necessary.

Individual access

Federal, provincial and territorial privacy laws grant individuals a right of access to their personal information, including that contained in audio and video recordings made using BWCs. This right is subject to specific exemptions such as law enforcement and investigation.⁹ Under freedom of information legislation, individuals have the right to request access to information held by public bodies. LEAs should establish a process for responding to requests for information contained in BWC recordings. When providing access, care should be taken to ensure that the personal information of individuals other than the requester, such as their image and/or voice, wherever possible, is protected.

⁸ At the federal level, please refer to Community Security Establishment's IT Security Guidance document "[Clearing and Declassifying Electronic Data Storage Devices](#)" and the OPC's "[Personal Information Retention and Disposal: Principles and Best Practices](#)." In Québec, please see the "[Guide to the destruction of documents that contain personal information](#)" published by the Commission d'accès à l'information du Québec.

⁹ Please address any questions about specific exemptions to the privacy oversight office in your jurisdiction.



Documenting policies and procedures


As part of any BWC program, LEAs should establish written policies and procedures that clearly identify the program objectives and set out the rules governing the program. These policies and procedures should include the elements listed below.

Governance and accountability

- The rationale for deploying BWCs, including the program purposes and operational needs.
- The legislative authorities for collecting personal information under the program.
- Roles and responsibilities of staff with regard to BWCs and their recordings.
- Criteria for context-specific continuous recording and/or turning BWCs on and off, as applicable.
- Provision for an operational guide and training for employees to ensure that officers understand the privacy implications of BWCs and are aware of their responsibilities under these policies and procedures.
- Privacy protections for employees whose personal information is captured by BWCs.
- The allocation of responsibility for ensuring that BWC policies and procedures are followed, with overall accountability resting with the head of the organization.
- The consequences of not respecting the policies and procedures.
- Individuals' right of recourse. Individuals should be informed that they have a right to make a complaint to the LEA's privacy oversight body regarding the management of a recording containing personal information to determine whether a breach of privacy law has occurred.
- The requirement that any contracts between LEAs and third-party service providers specify that recordings remain in the control of LEAs and are subject to applicable privacy laws.
- A provision for regular internal audits of the BWC program to address compliance with the policy, procedures and applicable privacy laws. The audit should include a review of whether BWC surveillance remains justified in light of the stated purposes of the program.
- In jurisdictions with a PIA policy, a provision for PIAs whenever there are significant modifications to the program.
- The name and contact information of an individual who can respond to questions from the public.

Use and disclosure of recordings

- The circumstances under which recordings can be viewed. Viewing should only occur on a need-to-know basis. If there is no suspicion of illegal activity having occurred and no allegations of misconduct, recordings should not be viewed.
- The purposes for which recordings can be used and any limiting circumstances or criteria, for example, excluding sensitive content from recordings being used for training purposes.
- Defined limits on the use of video and audio analytics.

- 
- The circumstances under which recordings can be disclosed to the public, if any, and parameters for any such disclosure. For example, faces and identifying marks of third parties should be blurred and voices distorted wherever possible.
 - The circumstances under which recordings can be disclosed outside the organization, for example, to other government agencies in an active investigation, or to legal representatives as part of the court discovery process.

Safeguards and response to breaches

- The security safeguards employed to ensure that recordings are not inappropriately accessed or altered.
- A mechanism for dealing with any breaches whereby personal information is accessed without authorization or disclosed contrary to the provisions of applicable privacy laws.

Access to recordings by individuals

- A process for responding to requests for access¹⁰ to recordings, including access to personal information and access to information requests under freedom of information laws, as well as individuals' requests for correction of their personal information. This includes the name and contact information of the individual to whom such requests for access to should be directed.

Retention and destruction of recordings

- Retention periods and disposal provisions.

These policies and procedures should be made available to the public to promote transparency and accountability. Demonstrating to the public that policies and procedures exist and officers are accountable for following them is essential to ensuring that individuals' privacy rights are adequately protected. The documentation should also reflect evidence of community consultation and engagement as well as an understanding of cultural sensitivities.

Conclusion

BWCs record not only the actions and speech of an individual, but also individuals' associations with others within recording range, including friends, family members, bystanders, victims and suspects. The recording of individuals through the use of BWCs raises a significant risk to individual privacy, and LEAs must be committed to only deploying BWCs to the degree and in a manner that respects and protects the general public's and employees' right to personal privacy.

¹⁰ LEAs should have the capability to redact third party personal information to facilitate access, for example, blurring of faces.



References

Tony Farrar and Dr. Barrar Ariel. [“Self-awareness to being watched and socially-desirable behavior: A field experiment on the effect of body-worn cameras on police use-of-force,”](#) Police Foundation, March 2013.

David A. Harris. [“Picture this: body worn video devices \(“Head cams”\) as tools for ensuring fourth amendment compliance by police,”](#) University of Pittsburgh School of Law, April 2010.

The Honourable Frank Iacobucci. [“Police Encounters with People in Crisis,”](#) An independent review conducted for Chief of Police William Blair, Toronto Police Service. July 2014.

Police Executive Research Forum. [“Implementing a Body-Worn Camera Program.”](#) U.S. Department of Justice, Community Oriented Policing Services, 2014.

Jay Stanley. [“Police Body-Mounted Cameras: With Right Policies in Place, a Win For All,”](#) ACLU, October 2013.

The Urban Institute Justice Policy Center. [“Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners,”](#) September 2011.

U.K. Home Office. [“Surveillance Camera Code of Practice,”](#) June 2013.

U.S. Department of Justice. [“A Primer on Body-Worn Cameras for Law Enforcement,”](#) Office of Justice Programs, National Institute of Justice, September 2012.

Public sector video surveillance guidance from Canadian privacy oversight bodies

Office of the Information and Privacy Commissioner for British Columbia. “[Public Sector Surveillance Guidelines](#),” 2014.

Office of the Information and Privacy Commissioner of Saskatchewan. “[Guidelines for Video Surveillance by Saskatchewan Public Bodies](#).”

Office of the Information and Privacy Commissioner of Ontario. “[Guidelines for the Use of Video Surveillance Cameras in Public Places](#),” 2007.

Commission d'accès à l'information du Québec. “[Rules for use of surveillance cameras with recording in public places by public bodies](#),” June 2004.

Office of the Access to Information and Privacy Commissioner of New Brunswick. “[Best Practice – Video Surveillance](#),” April 2014.

Office of the Information and Privacy Commissioner for Newfoundland and Labrador. “[Guidance for the Use of Video Surveillance Systems in Schools](#),” February 2013.

Office of the Information and Privacy Commissioner for Newfoundland and Labrador. “[Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador](#),” May 2005.

Nova Scotia Freedom of Information and Protection of Privacy Review Office. “[Freedom of Information and Protection of Privacy Review Office Video Surveillance Guidelines](#).”

Office of the Yukon Information and Privacy Commissioner. “[Guidance for Public Bodies on the Use of Video Surveillance](#),” 2014

Office of the Privacy Commissioner of Canada. “[OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities](#),” March 2006.