GENERAL

Updated January 2026

Public sector surveillance guidelines

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

PURPOSE OF THIS GUIDANCE DOCUMENT

The purpose of this guidance document is to provide information on how the *Freedom of Information and Protection of Privacy Act* (FIPPA) applies to the use of video and audio surveillance systems by public bodies. It also provides guidance on how public bodies should approach emerging technologies that often accompany modern surveillance systems, such as facial recognition technology (FRT) and artificial intelligence (AI) tools. These guidelines aim to assist public bodies in deciding whether proposed or existing surveillance systems are lawful and operating in a privacy-protective manner. The principles outlined in these guidelines can serve as useful starting points for public bodies considering a wide range of surveillance, including body-worn cameras, dash cams, drones or fixed cameras, such as on buildings or traffic poles. These guidelines also set out what the Information and Privacy Commissioner for British Columbia expects from public bodies who are considering using video and audio surveillance systems.

THE RIGHT TO PRIVACY

People living in British Columbia are increasingly subject to routine and random surveillance of their ordinary, lawful public activities by public and private bodies. Recent advances in technology have meant that high-quality, technologically advanced cameras are widely available and easily installed. As surveillance increases, so do the risks of harm to individuals. Video and audio surveillance systems are particularly privacy intrusive measures because they often subject individuals to continuous monitoring of their everyday activities.

Privacy is a fundamental right. Sections 7 and 8 of the *Canadian Charter of Rights and Freedoms* protect the rights of individuals to be secure in their daily lives and to be free from unjustified intrusion. FIPPA also recognizes and protects an individual's privacy rights and has been recognized as quasi-constitutional legislation. The protection of personal privacy has been referred to as a basic prerequisite to the flourishing of a free and healthy democracy by the Supreme Court of Canada.[1]

APPLICATION OF FIPPA AND ROLE OF THE OIPC

Public bodies may only collect, use, or disclose personal information if authorized under FIPPA. Except in very limited circumstances, public bodies must assume that video surveillance is capturing personal information given the detail and amount of information these systems record.

[1] *R v Jones*, 2017 SCC 60 at para 38, https://canlii.ca/t/hp63x#par38

Where a surveillance system records personal information, public bodies must comply with the privacy protection provisions in Part 3 of FIPPA and ensure they can meet their legal obligations for access to the records under the freedom of information provisions in Part 2 of FIPPA.

All public bodies are required to complete a privacy impact assessment (PIA) under s. 69(5.3) for any new initiative for which a PIA has not previously been done. The BC Government has full information and templates for PIAs online.[2] The Office of the Information and Privacy Commissioner (OIPC) can review and comment on draft PIAs for public bodies. There is no fee for an OIPC review. All public bodies are encouraged to consult the OIPC early on in any surveillance project to assist them in meeting their obligations under FIPPA.

The OIPC is responsible for monitoring and enforcing compliance with FIPPA and may conduct investigations and audits of public bodies' surveillance systems under the authority of s. 42(1)(a).

LAWFUL COLLECTION AND USE

Public bodies can only collect personal information in circumstances permitted by s. 26 of FIPPA. A public body must be prepared to demonstrate to the OIPC, with specific evidence, that one or more provisions of s. 26 of FIPPA authorize its proposed or existing collection of personal information by a surveillance system.

Each component of the surveillance system must comply with FIPPA. For example, if a public body is considering implementing a surveillance system that collects video and audio footage, it must be able to demonstrate the purpose and the legal authority for both. This includes evidence that supports how each component fulfils the purpose of the collection. Collection of other elements of personal information, such as biometric information using facial recognition technology, is considered a distinct collection and would similarly require specific legal authority.

Section 32 of FIPPA limits the purpose for which a public body can use personal information. Public bodies must be prepared to demonstrate how the ways they are using personal information meet the requirements of s. 32.

[2] See Government of British Columbia. "Privacy Impact Assessments." https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments

WHAT IS PERSONAL INFORMATION?

FIPPA defines "personal information" as recorded information about an identifiable individual, other than contact information. Video and audio recordings of an individual's image and voice are considered identifiable information.

Information is about an identifiable individual when it is reasonably capable of identifying a particular individual, either alone (direct identifiers) or when combined with other available sources of information (indirect identifiers).[3] Direct identifiers are specific pieces of information that are unique or nearly unique to an individual: for example, name, address, or faceprint.

Indirect identifiers are information that can, in combination with other available information, with a reasonable likelihood, point to an individual. Indirect identifiers must be understood in context to determine the extent to which they may be personal information. For example, an image of a black SUV in a large city is not likely to be personal information because it is an exceedingly common vehicle in a location in which there are many other vehicles matching that description. However, an image of a customized yellow sports car may be identifiable personal information in a small town where it is likely the only such vehicle, or when it's captured travelling to or from a particular residence. Collection of information about such a vehicle is reasonably likely to be tantamount to direct collection of information about its owner.

WHAT IS COLLECTION?

In terms of surveillance systems, collection of personal information occurs when an individual's personal information is captured by the system. The personal information may then be played back or displayed on a monitor (used), saved or stored (retained) or shared with other public bodies or organizations (disclosed). Surveillance systems are always collecting personal information regardless of if, or how, the public body uses, retains or discloses that personal information in the future.

26(a): Collection expressly authorized by the Act

Section 26(a) of FIPPA allows for the collection of personal information that is "expressly authorized under an Act." This is the most straightforward legal authority for collection.

[3] See BC OIPC. October 2025. Order F25-86: Vancouver Coastal Health Authority, at para 11, https://www.oipc.bc.ca/documents/orders/3045, citing BC OIPC. September 2005, Order F05-30: Corporation of the City of New Westminster, at para 35, https://www.oipc.bc.ca/documents/orders/855.

However, there are specific requirements:

- The authorization must be under an "Act," which means an Act of the Legislature;[4] and
- The authorization must be "expressly" authorized in that Act, which means permitting the specific method and circumstances of the collection of personal information.[5]

If there is an authority under an Act that states that a public body is authorized to collect personal information using video or audio recording, then, so long as the collection is done in accordance under that Act and for the specified purpose, it is authorized.

An example of express statutory authority for video surveillance is found in s. 85 of the *Gaming Control Act*. Under this section, the British Columbia Lottery Corporation "may place a gaming site under video surveillance to ascertain compliance" with the Act. Section 74.01 of the *School Act* similarly expressly authorizes the use of surveillance cameras by a school board under certain conditions.[6]

S. 26(b): Collection for the purposes of law enforcement

Section 26(b) of FIPPA authorizes collection of personal information for the purposes of law enforcement. Schedule 1 of FIPPA defines "law enforcement" as: policing, including criminal intelligence systems; investigations that lead or could lead to a penalty or sanction being imposed; or proceedings that lead, or could lead, to a penalty or sanction being imposed.

"Policing" is not defined in FIPPA, but has been interpreted by the OIPC to mean "activities carried out by a police officer under a statutory or common law authority."[7] Information collected for policing purposes must be collected by a public body with a common law or statutory enforcement mandate. For example, it is not sufficient for a public body to claim an interest in reducing crime to justify collection for "law enforcement." Instead, the public body must have a common law or statutory law enforcement mandate to enforce those laws.

For example, in Investigation Report F26-01, the OIPC determined that s. 26(b) does not authorize the City of Richmond to collect personal information using video surveillance for the purpose of policing, because the City does not have a mandate to police individuals.

In addition, to rely on this section an investigation must already be underway at the time the personal information is collected for s. 26(b) to apply. A public body is not authorized to collect personal information about individuals, in the absence of an investigation, on the chance it may

---

[4] *Interpretation Act*, RSBC 1996, s. 1.
[5] See BC OIPC. July 2014. Order F14-26: Ministry of Justice, paras 21-28, https://www.oipc.bc.ca/documents/orders/1589.
[6] *School Act*, RSBC 1996, c 412, s.74.01, https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96412_06#section74.01
[7] BC OIPC. March 2025. Order F25-23: Vancouver Police Department, at para 85, https://www.oipc.bc.ca/documents/orders/2940

be useful in a future investigation. Similarly, in order for a collection to be lawfully authorized as relating to a proceeding, the proceeding must be ongoing at the time of collection.

Section 26(c): Collection of personal information that is necessary for a program or activity of the public body

To rely on this section, a public body must be able to demonstrate that the personal information it is collecting is for a purpose that is related directly to a defined program or activity that is within the public body's mandate, and that the personal information the public body collects is necessary (as opposed to helpful or convenient) to achieve that purpose.

Section 26(c) recognizes that an authorized program or activity may require the collection of personal information. If a public body can show that collection is necessary for its authorized program or activity, the collection is authorized under s. 26(c). To evaluate whether s. 26(c) authorizes a public body to collect personal information, the OIPC recommends public bodies break down their assessment into these four steps:

1. Define the program or activity of the public body

The public body must define the program or activity that it is engaged in to determine whether that program or activity is an authorized one, and whether the collection of personal information relates directly to it. OIPC Orders have interpreted a "program" for the purposes of this section as being "an operational or administrative program that involves the delivery of services under a specific statutory or other authority," or a "designed delivery of services to more than one individual."[8] An "activity" means an action that is taken in pursuit of an objective.

2. Establish that the program or activity is within the public body's mandate

FIPPA's purposes include "preventing the unauthorized collection, use or disclosure of personal information by public bodies."[9] The public body must identify what mandate the program or activity falls within, being careful to make sure the program or activity does not fall outside the bounds of what their mandate permits. The source of the public body's mandate varies by public body but can include an Act, a regulation, a mandate letter[10] or the common law.[11] Only those programs or activities that fall within

[8] BC OIPC. October 2019. Order F19-37: Ministry of Finance, paras 27-28, https://www.oipc.bc.ca/documents/orders/2214.

[9] FIPPA, s. 2(1)(d).

[10] Not all public bodies have mandate letters. Mandate letters for Cabinet Ministers and for Crown Corporations are usually published online annually. See, for example, Government of British Columbia. "Executive Council and Parliamentary Secretaries of B.C." https://www2.gov.bc.ca/gov/content/governments/organizational-structure/cabinet/cabinet-ministers, and Government of British Columbia. "Mandate letters for Crown Corporations." https://www2.gov.bc.ca/gov/content/governments/services-for-government/public-sector-management/plan-report/crown-corporations/mandate-letter

[11] BC OIPC. January 2026. Investigation Report 26-01: Investigation of City of Richmond's Public Safety Camera System Field Test. https://www.oipc.bc.ca/documents/investigation-reports/3073

a public body's mandate will meet this requirement. A public body cannot define a program or activity broadly and in a way that is outside of its mandate to authorize a collection of personal information.

3. Determine whether the personal information the public body seeks to collect is directly related to that program or activity

A public body must be able to demonstrate that the collection of the personal information relates directly to the program or activity. For example, the Ministry of Finance collects property owners' names and addresses to levy taxes for which they are liable and that the public body is lawfully permitted to collect.[12]

A public body will still need to show that the program or activity itself falls within its own mandate, even if the collection directly relates to the program or activity.

4. Determine whether the collection is "necessary"

Whether collection of personal information is "necessary" for a program or activity of a public body needs to be assessed in a rigorous way. While this is a high standard, it is not so strict to mean that information will only be found to be necessary where it would be "impossible" to operate that program or activity. On the other hand, it is not enough for the information to be "nice to have."[13] To evaluate whether the collection of the personal information is necessary, a public body must examine in detail the types of information being collected and determine whether each type is truly necessary for the program or activity.[14]

The OIPC recommends that public bodies start by considering the following factors in determining whether collection of personal information by surveillance is "necessary" for the purposes of s.26(c):

- **The sensitivity of the personal information:** A public body must consider that sensitivity can be related to the volume of the information collected, the resolution of images collected. For example, can individual features be discerned, can phone screens be read, or can other information be deduced by the location of the camera, such as in front of a workplace, a place of worship, etc. Newer technology can capture very detailed information at a distance, including biometric information, which is always highly sensitive personal information.

[12] See BC OIPC. October 2019. Order F19-37: Ministry of Finance, at para 47, https://www.oipc.bc.ca/documents/orders/2214

[13] BC OIPC. June 2007. Order F07-10: The Board of Education of School District No. 75 (Mission), paras 48-49, https://www.oipc.bc.ca/documents/orders/885

[14] See BC OIPC. January 2026. Investigation Report 26-01: Investigation of City of Richmond's Public Safety Camera System Field Test, p 30, https://www.oipc.bc.ca/documents/investigation-reports/3073, citing *Cash Converters Canada Inc. v. Oshawa (City)*, 2007 ONCA 502 (CanLII), at para 41, https://canlii.ca/t/1rxpx

- **The particular purpose for the collection:** The OIPC expects the public body to consider whether the problem it seeks to address using surveillance is real, substantial, and pressing. Further, they must determine whether there are other, less intrusive means of achieving the same purpose that are as effective as surveillance for the program or activity.
- **The amount of personal information collected, assessed in the context of the purpose for the collection:** A public body must consider whether the benefits of video surveillance substantially outweigh the reduction of privacy inherent in its use.
- **Whether the collection adheres to the principle of data minimization:** Data minimization means only collecting an amount of personal information that is required to fulfil the purpose, and nothing more. A public body must scrutinize its proposed collection of personal information for a program or activity and evaluate whether it is adhering to this principle.[15]

Section 26(c) is the broadest collection authority in FIPPA, recognizing that public bodies need to collect information about individuals to discharge their mandates while simultaneously placing limits on the scope of that collection. If a public body uses this source of authority for collection there is that much more of an onus to limit scope, demonstrate necessity and be transparent.

Public bodies relying on this section to authorize collecting personal information through surveillance are strongly encouraged to seek guidance from the OIPC early in their project planning.

WHAT ABOUT CONSENT?

Under s. 26(d) of FIPPA, consent can be used as legal authority for the collection of personal information for very few prescribed purposes.[16] Express or implied consent is not a legal authority for the collection of personal information using video or audio surveillance systems.

This underscores one of the fundamental differences between FIPPA and the private sector *Personal Information Protection Act* (PIPA).

[15] BC OIPC. January 2026. Investigation Report 26-01: Investigation of City of Richmond's Public Safety Camera System Field Test, p 32, https://www.oipc.bc.ca/documents/investigation-reports/3073 citing *Cambridge (City) (Re),* 2021 CanLII 37668 (ON IPC), at paras 40-41, https://canlii.ca/t/jfrxh

[16] Freedom of Information and Protection of Privacy Regulation, BC Reg. 248/2022, s. 9. https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/155_2012#section9

PIPA is a consent-based statute: organizations in the private sector can only collect, use or disclose someone's personal information with their consent. PIPA's consent requirements give people control and choice.

That same level of choice is not practical in the public sector, which provides services that are essential to everyday life – healthcare, education, infrastructure – and for which there is limited choice or ability to opt out. Consent is not viable where there is no real choice, which is why FIPPA is an authority-based statute: public bodies need legal authority to collect personal information. The responsibility to protect privacy rests with the public body, not the individual. This is why public bodies must have express authority to collect personal information, why the safeguards in FIPPA are strong, and why the OIPC expects public bodies to meet a high standard.

EFFECTIVE AND AUTHORIZED USE OF SURVEILLANCE

Information collected through surveillance must not be used beyond the original purpose for the collection, and not any other purpose that is demonstrably inconsistent with this purpose. Collecting personal information for one purpose, then using it for another is an example of "function creep," which can lead to public bodies using personal information in ways that do not meet the requirements of FIPPA. For example, a public body would not be authorized to install a camera for security purposes and then retain and use the footage to audit employee attendance.

Public bodies may only use personal information if one of the provisions listed under s. 32 is met.

A public body may only use a video or audio surveillance system where conventional means for achieving the same objectives are substantially less effective than surveillance, and the benefits of surveillance substantially outweigh any privacy intrusion. Cost savings alone are not sufficient justification to proceed with a surveillance system under FIPPA.

AUTHORIZED DISCLOSURE OF VIDEO SURVEILLANCE

Public bodies must similarly establish a legal authority in FIPPA for disclosing personal information; otherwise, they must not disclose it. FIPPA provides several authorities for disclosing personal information, including responding to an access request (discussed later in this guide), in the public interest within the meaning of s. 25 or most commonly for a purpose authorized by s.33.

There are many disclosure authorities under s. 33 of FIPPA but those commonly used for video surveillance include:

- for the purpose the information was collected or a consistent purpose (33(2)(d));
- to support a specific law enforcement investigation (s. 33[3][d]);
- to comply with a subpoena, warrant or court order (s. 33[2][l];
- with written consent in the manner set out in FIPPA's Regulations (s. 33[2][c]);

A public body seeking to disclose personal information collected using surveillance must review the authorities to see if one applies to the situation. If one does apply, the public body must then consider whether to exercise discretion to disclose that information, as all disclosures under s. 33 of FIPPA are discretionary. Particularly where disclosure is regular, ongoing or systematic, a public body must develop policies and procedures to ensure any disclosure is authorized, secure and privacy protective.

SURVEILLANCE — ROAD MAP

1. The OIPC advises public bodies to take the following steps when considering whether to implement a surveillance systems:

(a) Complete a PIA before implementing a surveillance system. This is not only required under FIPPA, but is an important component in the design of a project to assess how the project affects the privacy of individuals, and must include a description of measures to mitigate any identified privacy risks. The OIPC strongly encourages public bodies to send the office a copy of the completed PIA, including the public body's case for implementing a surveillance system as opposed to other measures, for review and comment. The OIPC should be consulted in the design phase and well before any final decision is made to proceed with surveillance.

(b) If a public body would like to use surveillance for security reasons, it must have evidence, such as verifiable, specific reports of incidents of crime, public safety concerns or other compelling circumstances that support the necessity of surveillance.

(c) Conduct consultations with stakeholders who may be able to help the public body consider the merits of the proposed surveillance.

(d) Calibrate the surveillance system so that it only collects personal information that is necessary to achieve the purposes the public body has identified for the surveillance.

2. In designing and implementing a surveillance system, the OIPC advises public bodies to:

(a) Install surveillance equipment such as video cameras or audio recording devices in defined public areas. The public body must select areas it expects the surveillance will be most effective in meeting the purpose for the surveillance.

(b) Recording equipment must not be positioned, internally or externally, to monitor areas outside a building, or to monitor other buildings, unless necessary to accomplish the purpose for the surveillance. Cameras must not be directed to look through the windows of adjacent buildings. Equipment must not monitor areas where the public and employees have a reasonable expectation of privacy, such as change rooms and washrooms.

(c) If the purpose of the surveillance is related to crime, the public body must restrict the use of surveillance to periods when there is demonstrably a higher likelihood of crime being committed and detected in the area under surveillance.

(d) Section 27(2) of FIPPA requires that, in most circumstances, a public body must notify individuals when they are collecting personal information. A public body must notify the public, using clearly written signs prominently displayed at the perimeter of surveillance areas, so the public has sufficient warning that video or audio surveillance is or may be in operation before entering any area under surveillance. The notification must state: the purpose for the collection, the legal authority for the collection, and the title, business address and business telephone number of an employee of the public body who can answer the individual's questions about the collection.

(e) Only authorized individuals should have access to the system's controls and to its reception equipment, such as video monitors or audio playback speakers. Public bodies must have policies and protections in place to ensure that only authorized individuals access personal information from a surveillance system for authorized purposes.

(f) Recording equipment must be in a controlled access area. Video monitors must not be located in a position that enables public viewing. Only authorized employees should have access.

3. Guidelines regarding surveillance records

(a) **Security of records**
Section 30 of FIPPA requires that a public body protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, access, use, disclosure or disposal. OIPC guidance

documents outline reasonable security safeguards, which include but are not limited to:[17]

- risk management programs;
- written privacy and security policies;
- physical and technical security protocols;
- role-based access controls;
- retention schedules; and
- incident management response plans.

Public bodies must consider potential risks and the likelihood of damage or harm in the event of an incident when evaluating safeguards.

An additional consideration with surveillance records relates to where the records will be stored and the corresponding security risks. Public bodies must determine whether they will store the personal information:

- in one physical location they own and maintain (this is sometimes called on premise);
- in a fluid location on different pieces of equipment they own and maintain (sometimes called a local cloud);
- or on equipment owned and maintained by a third party (sometimes called cloud computing).[18]

Public bodies must be particularly mindful of ensuring they meet their security obligations when using third-party service providers for cloud storage outside of Canada. For further information see OIPC guidance on this subject.[19]

With surveillance cameras specifically, cheaper is not necessarily better. The camera technology itself may be the least expensive part of a surveillance program.

---

[17] The OIPC has several guidance documents about security. See in particular, BC OIPC. October 2020. Securing personal information: a self-assessment for public bodies and organizations. https://www.oipc.bc.ca/documents/guidance-documents/1372

[18] The Canadian Centre for Cyber Security defines cloud computing as: "The use of remote servers hosted on the Internet. Cloud computing allows users to access a shared pool of computing resources (such as networks, servers, applications, or services) on demand and from anywhere. Users access these resources via a computer network instead of storing and maintaining all resources on their local computer." See Canadian Centre for Cyber Security. Glossary. https://www.cyber.gc.ca/en/glossary#c

[19] BC OIPC. March 2022. Reasonable security measures for personal information disclosures outside Canada. https://www.oipc.bc.ca/guidance-documents/3646

(b) **Retention of records**

With any surveillance recordings, public bodies should establish a records retention and destruction schedule and have it approved by the head of the public body.

If the recorded information reveals an incident that contains personal information about an individual, and the public body uses this information to make a decision that directly affects the individual, s. 31 of FIPPA requires that specific recorded information be retained for one year after the decision is made, so that the affected individual has a reasonable opportunity to obtain access to that personal information.

For recordings not used in a decision, public bodies must only keep personal information for as long as they need it to fulfil the purpose for which it collected it. This might mean, for example, that a public body deletes personal information collected using surveillance in as little as 24 hours after collecting it. Keeping personal information for longer than a public body needs it is an unnecessary security risk.

(c) **Access to records**

Only authorized individuals who require the information to do their jobs should have access to the surveillance system or the records it creates. All authorized personnel must be fully aware of the purposes of the system and fully trained in rules protecting privacy. Logs must be kept of all instances of access to, and use of, recorded material.

An individual who is the subject of surveillance has the right to request access to their personal information under s. 5 of FIPPA. This is commonly known as a "freedom of information" or FOI request. FIPPA requires public bodies to withhold personal information about other individuals if disclosing that information would unreasonably invade their privacy. Other sections of FIPPA either require or authorize a public body to refuse access to information. Practically, a public body must have the means to blur or otherwise obfuscate the identity of other individuals on a recording before responding to an FOI request, subject to what is reasonable.[20]

Public bodies must have trained employees who can search for records, surveillance or otherwise, review them for statutory exceptions to access, sever or exempt information, and respond to the requestor. Lacking the capacity to blur or sever information to respond to an FOI request is not a valid reason under FIPPA to excuse a public body from performing this task. Public bodies must have the technical capacity, sufficient human resources, and the appropriate policies and procedures in place to conduct such processing within the timeframes specified by FIPPA prior to commencing any

[20] For a discussion of the limits of what is reasonable to sever with respect to surveillance recordings, see BC OIPC. February 2024. Order F24-10: Metro Vancouver Transit Police, https://www.oipc.bc.ca/documents/orders/2754. In that order, the public body blurred some information, and the adjudicator found that the public body was not required to further blur or obfuscate other information.

information collection through surveillance. If a public body does not have the human resources or technical capacity to meet their FOI obligations under FIPPA then this will impact the ability to implement the surveillance. Public body programs must be designed to accommodate this right to seek access.

(d) Ongoing evaluation

The effectiveness of a video or audio surveillance system must be regularly evaluated, including by independent evaluators. Some considerations for evaluation include:

- Taking special note of the initial reasons for undertaking surveillance and determining whether video surveillance has addressed the problems identified.
- Reviewing whether a video or audio surveillance system should be terminated, either because the problem that justified its use in the first place is no longer significant, or because the surveillance has proven ineffective in addressing the problem.
- Taking account of the views of different groups in the community (or different communities) affected by the surveillance.

Results of evaluations should be made publicly available.

Public bodies are expected to review their PIA annually, at a minimum, and update it if their operational needs change and they need to expand or discontinue the surveillance, if the signatories to the PIA need to be updated, or if there is a change to the legal basis on which the public body relies for their authority to conduct the surveillance.

CONCLUSION

Video and audio surveillance systems are inherently privacy invasive. For a public body to use surveillance, it must first establish that FIPPA authorizes the use. Even if surveillance is authorized, a public body should determine whether there are other, less privacy invasive options available.

For further information, please visit our website at www.oipc.bc.ca or contact:

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038 Stn Prov Govt
Victoria BC, V8W 9A4
Email: info@oipc.bc.ca
Phone: (250) 387-5629

Callers outside Victoria can contact the office toll-free by calling Service BC and requesting a transfer to (250) 387-5629.

Service BC: Vancouver: (604) 660-2421; Elsewhere in BC: (800) 663-7867